Global Information Assurance Certification Paper

Michael Cullen

“Securing Windows 2000 Server for Mobile Local Area Networks”

Certified Windows Security Administrator (GCNW)

Practical Assignment Version 3.1 (revised April 8, 2002)

Option 2 – Securing Windows 2000 with Security Templates

May 2003

Table of Contents

Abstract

As computer security continues to grow as a large area of focus for organizations many templates/checklists have been created and published to the World Wide Web. Most of these tackle the issue of security for the Microsoft Windows operating systems. This paper recounts researching these templates/checklists, choosing one template and applying it to a stand alone Windows 2000 Server system. After the application, a series of security settings tests and functionality tests were run to help evaluate the effectiveness and impact the template has on

the test environment. Finally recommendations for improvements and future manageability of the template were made.

Introduction

As more organizations deploy laptops to end users the work force becomes more mobile. With this portability come many different logistical and security challenges. One such challenge is the ability to share knowledge while "in the field". Many types of businesses, such as consulting, accounting, auditing, other contracting, provide services to their clients on site. On site may be at the client's office, a hotel, a factory/plant, or almost any location where the client conducts their business. These projects can last from a couple of days to months and, in some cases, involve large teams of people.

For a number of reasons these teams may need to share files, applications, and printing capabilities and many times it is not practical or advisable to use the client's resources, especially a connection to the Internet. To solve this problem many organizations deploy mobile local area networks (LAN). These networks consist of a stand alone server (usually a laptop or small form factor desktop), a printer, and a switch/hub. Mobile LANs provide these service providers with the resources to maintain control over their data and applications while also allowing the team to share information securely.

To constrain the scope of the practical the mobile LAN server belongs to an accounting firm that performs financial statement auditing and financial consulting. To conduct the audit the firm will send its accountants to the client's location(s). Many times the auditors are under time pressure to complete the audit in a short amount of time usually less than 60 days. This short deployment time for the mobile LAN allows for a more secure environment, there are fewer opportunities for security breaches. With a longer deployment more stringent requirements would be needed to maintain the same level of security.

Description of System

The stand alone server for the mobile LAN served three basic roles, file sharing, printer sharing, and Dynamic Host Configuration Protocol (DHCP) addressing. For file sharing a single folder was shared allowing users to create their own folder structure depending on the type of project being completed. A single printer was shared for all users to access. Also, Internet Protocol (IP) addresses were assigned by the server to all other network devices.

The server is stand alone for a number of reasons. First, it must be mobile since the engagement team requires flexibility. A server that must always be connected to a network limits the team's functionality. Second, not every client environment will have an Internet connection. Even if the connection is available, for security purposes the client doesn't want a foreign system on their network

that must communicate through their firewall. Finally, attaching the server to any network immediately increases the chances that the confidential data on the system could be compromised.

Hardware Specifications

A laptop was chosen as the mobile LAN server more many reasons. Unlike a desktop it can be easily transported to and from the client site daily, has all the necessary components built in (i.e., monitor, keyboard), and it takes up relatively little space. The major specifications for the server's hardware are listed below.

Brand	IBM ThinkPad
Model / Type	T30 / 2366-21U
Processor	Mobile Pentium 4 1.6 GHz
Memory	256 MB
Hard Drive	20 GB
Main board Chipset	Intel 82845
Networking	Intel PRO/100 VE
Modem	Lucent Soft Modem AMR
Optical Drive	Hitachi DVD-ROM

Software Setup

Since the server had to allow file sharing, printer sharing, and the assignment of IP addresses Windows 2000 Server was chosen. Windows 2000 Professional could not be used because it is limited to ten (10) concurrent connections at a time. This would not be acceptable when the project team consisted of more than ten people. Also, the professional edition does not have a DHCP server built into the operating system. Without DHCP capabilities IP addresses would have to be manually configured on each network device (i.e. computers, printers).

The first step was to install Windows 2000 Server on the laptop. Immediately following this, installation drivers for the network card, modem, TrackPoint, and power management features were installed. The drivers were downloaded from the IBM support web site. Next, the system was updated with Windows 2000 Service Pack 3. Then, using the Microsoft Windows Update web site other miscellaneous patches and fixes were installed, including Internet Explorer 6.

After completing those updates the Microsoft Baseline Security Analyzer (MBSA) was installed. It reported three more patches that needed to be applied. After those final patches were applied, MBSA reported no patches were missing (see Figure 1 below). Norton Antivirus Corporate Edition 7.6 was installed to provide virus protection on the server. It was updated using Norton's LiveUpdate software with the latest virus definitions.

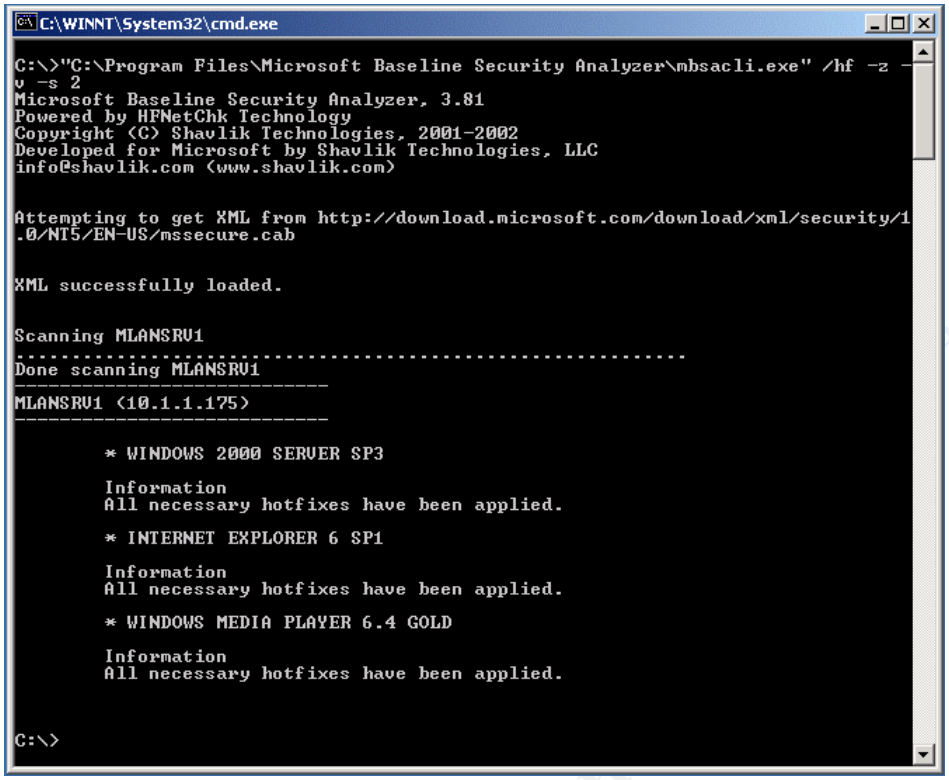

Figure 1

Due to the nature of the practical the application of the template is covered later. However, to conclude the software setup section we must talk about standardizing the software setup. The best way to accomplish this is by using Norton Ghost to create an image of the system. This image can then be used to quickly setup more mobile LAN servers because all of the manual steps above would be replaced by the simple process of imaging the new system. The creation of the image should only occur after the entire setup process is complete; in this case after the security template is applied and fully tested. Using Ghost to create the image and standardize the deployment is great, but there is one drawback, updating. If updates to the security patches on the system or changes to the security template are needed either a new image must be created and deployed or each mobile LAN server must be manually updated. This might be fine for a small number mobile LAN servers, but as the number systems grows, a more automated and efficient process for updating the system will be needed (This topic is covered later in the paper).

Another software setup task that would be completed after the security template is supplied, but fits better in this section of the practical is user provisioning. After the security template is applied (or in future cases after the systems has been setup with the appropriate image) users must be added to the server. The technology support group setting up the mobile LAN receives a mobile LAN server request form. On this form is a list of the employees who will be using the system in the field. The technical support technician (the Administrator) then

adds accounts and creates passwords for those users on to the mobile LAN server. The user name is based on the accountant's name. The password is assigned by the Administrator. The Administrator also sets the account properties to restrict the user from changing the password and requiring the user to change the password at next logon. The reasons the administrator assigns passwords are to ensure that the passwords meet the complexity standards and to keep the users from using the same user name and password combination they use on the companies network. This is done in case the mobile LAN server is stolen and some one gains access to the user names and passwords stored on the system. If they get access to that information they can use it to gain access to the accounting firm's systems causing major problems for the firm and it clients.

Workstation Security

For the purpose of this practical the security of the workstations that will be connecting to the mobile LAN and its server is out of scope. Including the details of their security settings would require another entire paper. However, since they are an important part of the mobile LAN environment the following brief overview of these systems is included.

The workstations are similar laptops to that of the mobile LAN server (see specifications above). They are running Windows 2000 Professional with the standard office applications, internet and email clients, and antivirus software. These machines are designed to log onto a Novell NetWare network and as such use the Novell NetWare Client for Windows. The entire accounting firm's network architecture is based entirely on NetWare. When users are away from the firm's offices they use the workstations in stand alone mode. They will use this same mode when connecting to the mobile LAN. The users have limited Administrative rights to their workstations.

Security Threats

The mobile LAN server concept provides a number of positives for the company; however, there are also a number of security threats. The major threat to the mobile LAN server is unauthorized access to client data. Since we are dealing with financial number of companies that end up in annual reports and are used by investors, regulators, and many others data security is by far the primary concerns. There are also secondary threats such as unauthorized access to proprietary tools and methodologies, use of the server for launching attacks against others, and theft. The major threat, unauthorized access to client data, will mainly be mitigated by the controls and settings implemented through the security template. Other threats are mitigated by not being connected to the Internet and by having the entire LAN (server, printer, switch/hub, clients) located in one room.

Security Requirements

The following security requirements were identified for the mobile LAN server based on its roles as file, print, and DHCP server. The firm does not have an official security policy, therefore these requirements are based solely on the threats stated above and common information security practices.

First, as a file server, these requirements must be met:

- Authorized users may only have access to the shared data folder
- Unauthorized or guest users may not have any access
- Only the Administrator may log into the system locally
- Authorized users may create subfolders in the shared data folder

Second, as a print server, these requirements must be met:

- Only authorized users may connect to the shared printer
- Authorized users may have full control over print jobs (this reduces the need for a user to have Administrator rights to control the printer queue)
- Only the Administrator may install and upgrade print drivers

Third, as a DHCP server, these requirements must be met:

- Only a small block of IP addresses can be assigned (there is no need to have an entire class C subnet available if only 20 users will be connected at a time)
- Only the Administrator may manage the DHCP server
- A small group of addresses in the subnet must be reserved for the server, printer, and future needs (i.e. additional printers, Internet router)

Finally, a number of general requirements must be met, a few of those are:

- All non-essential services must be disabled
- Windows logging must be enabled and logging access to all resources
- Windows auditing must be enabled
- The server must be secured using a lock down cable
- No remote access should be allowed to any directory except the shared folder
- Users should not be allowed to install applications on the server
- No dial-up access should be allowed

Access to the server will be limited to only members of the project team (the end users) and a system Administrator. The system Administrator will not be on site with the team, rather this person will set up the server before the project. Then after the job ends the Administrator will backup the client data on the server and redeploy the machine. The end users will only access the server through the mobile LAN. This limits exposure to the machine and increases security. Also, the lack of an Internet connection also means no remote connections are possible.

Choosing the Template

After researching the myriad of security templates available today, the template best suited for this server is the Win2kSrvGold_R1.0.inf provided by The Center for Internet Security (CIS). This template was chosen for a number of reasons. First, CIS has spent time developing this template by using the templates of the National Security Agency (NSA), Defense Information Systems Agency, and National Institute of Standards and Technology as a baseline. These templates provide a good starting point and by essentially combining the best of each template the CIS template should be the most comprehensive. Second, the CIS template is not designed for domain controllers. Since this system will not be a domain controller the extra security settings needed for that type of system are not present in the CIS template. Third, by using a brand name template that is well known the mobile LAN server system can be better sold to clients. When the accounting firm makes sales presentations it can emphasize the use of the CIS template as another way the firm keeps client data secure and confidential. Another reason for using this template is its approval by the General Services Administration, making it suitable for use on Federal Government contracts a key area of business for the accounting firm.

Based on the role of this server, the Win2kSrvGold_R1.0.inf template should provide very good security. The mobile LAN server was not designed to perform many complex tasks. Since the major amount of work the server will perform is serving files and managing printing this template's settings should be more than adequate. If anything, there is a possibility that template could be too strong for the server. In this sense too strong means that the added security might put restrictions in place that hamper the functionality of the system. Although, the added strength will probably not prohibit the needed functionality it may require more manual configuration at setup.

Security Settings

The security configuration for Windows 2000 is divided into seven main areas: Account Policies, Local Policies, Event Log, Restricted Groups, System Services, Registry, and File System. Although the CIS template makes changes to all of these areas not all changes are relevant to the configuration of the mobile LAN server. Listed below are the settings and their descriptions that are significant to this environment.

Account Policies

This section describes the policy settings for passwords and account lockout. Kerberos policies are also included in this section of the Windows security configuration but not addressed in the CIS template.

The first policy is ‘Enforce password history’ and its template setting is ‘24 passwords remembered’. This setting forces the system to keep a record of the last 24 password used by a user. This prevents users from reusing the same password or small set of passwords in rotation. This policy is not very relevant to the mobile LAN server, since users can’t change their passwords. But it is important for understanding how all of the password policies work together.

The next policy is ‘Maximum password age’ and its template setting is ’90 days’. This setting requires users to change their password at least once every 3 months. This allows users to keep the same password for a decent length of time, but keeps the user from using the same password indefinitely. In this environment most mobile LAN deployments last no more than 60 days meaning this setting should never impact the server or users. But again this setting is important in the understanding of the password policies.

The next policy is ‘Minimum password age’ and its template setting is ‘1 days’. This setting requires users have a password for a least one day before changing it. Again, it is not very relevant to this environment but important for understanding how all password policies work together to achieve the security requirements.

The next policy is ‘Minimum password length’ and its template setting is ‘8 characters’. This setting requires that the password is at least eight (8) characters long. This complexity makes it harder for an intruder to guess the password or use automated tools to break the password. This setting is very relevant to the environment and is possibly the most important password setting. To mitigate the risk of unauthorized access to client data requiring an 8 character minimum length on passwords mean a would-be intruder would need to expend a lot of resources, mostly time, to try to break the password.

The next policy is ‘Passwords must meet complexity requirements’ and its template setting is ‘Enabled’. This setting requires the password to contain more than just lowercase text. The password must have characters from three of the four types of characters: lower case, upper case, special characters (i.e. *, $, @), and numeric. By enabling this setting the administrator is forced to follow the rules above when setting up the passwords for the mobile LAN server’s users. This is very relevant to the environment since this password is the main control standing in the way of accessing the client’s data.

The next policy is ‘Store password using reversible encryption for all users in the domain’ and its template setting is ‘Disabled’. This setting, if enabled, allows password to be decrypted. This policy should probably only be enabled when required by certain applications. Reversible encryption makes it easier for intruders to decrypt passwords.

The next policy is ‘Account lockout duration’ and its template setting is ’15 minutes. This setting forces the system to deactivate a user account for 15 minutes after the number of invalid logon attempts has been met. This setting is not very relevant to this environment.

The next policy is ‘Account lockout duration’ and its template setting is ‘3 invalid logon attempts’. This setting sets the number of invalid logon attempts a user can have before the account is locked out. This setting provides protection against basic intruders trying to log into the system locally. Since our users are only accessing the server’s resources over the network this setting won’t have a direct impact on them.

The next policy is ‘Reset account lockout counter after’ and its template setting is ’15 minutes’. This setting resets the lockout threshold counter after 15 minutes. This policy is also not very relevant to this environment.

Local Policies

This section describes the settings for auditing, user rights, and security options. The first part of this section details the auditing policies for the server. In the mobile LAN environment these policies serve as a historical record that would only be reviewed in cases where the server was improperly accessed or not working properly. In a typical network environment these auditing settings are crucial to a network administrator’s day to day tasks. They allow the administrator to easily trace back problems to their root causes. This auditing, in connection with a system of notification, allows administrators instant alerts to problems with the system. However, in our mobile LAN environment no one will be monitoring these events. They will only be reviewed when the server is returned to technical support making them low relevance.

Auditing Policy	**Computer Setting**	**Explanation**
Audit account logon events	Success, Failure	Records all account logon events (remote, locally, batches, etc.) in the event log no matter if it is a success or failure.
Audit account management	Success, Failure	Records all account management events (changing passwords, creating users, renaming users, etc.) no matter if it is a success or failure.
Audit logon events	Success, Failure	Records all logon events in the event log no matter if it is a success or a failure.

Auditing Policy	Computer Setting	Explanation
Audit object access	Failure	Records only failed attempts of users to access objects (files) in the event log. Only failures are records due to the volume of data collected if even successful access attempts are made.
Audit policy change	Success, Failure	Records only failed attempts to change the audit policy in the event log.
Audit system events	Success, Failure	Records ALL system events in the event log no matter if it is a success or a failure.

This section, User Rights, of the Local Policies is very relevant and important to the mobile LAN environment. The settings determine what users and groups can do on the system.

The first policy is 'Access this computer from the network' and its template setting is 'Administrators, Users'. This setting only allows members of the Administrators and Users groups to access this system over the network. This is crucial to the operation of the environment. When users are provisioned on the mobile LAN server they are assigned by default to the Users group. With this policy in place only the members of those groups can access the system.

The next policy is 'Back up files and directories' and its template setting is 'Administrators'. This setting restricts the task of backing up data to the Administrators group. This is important for the server because once it is returned to technical support the technicians backup all of the client data to the firm's storage network.

The next policy is 'Bypass traverse checking' and its template setting is 'Users'. This setting allows the Users group to traverse the directory structure even though they don't have permission to access all folders in the structures. Since users can create subfolders in the server's shared directory and change their permissions to restrict access from other team members this setting must be enabled. This allows all of the team members, who are member of the Users group, to see what is out there on the system.

The next policy is 'Change the system time' and its template setting is 'Administrators'. This setting only allows the Administrators group to change the system time. This is important in maintaining valid log files and ensuring

scheduled jobs run properly. If any users could change the system time on the mobile LAN server is would cause problems for the logging functions and any scheduled jobs. Intruders can also use the functionality to commit crimes against the computer and then change the time so either new events will overwrite the logs of the improper acts or so scheduled jobs can be used to perform more harm in the future.

The next policy is 'Deny access to this computer from the network' and its template setting is 'Guests'. This setting restricts network access to the system from any members of the Guests group. Again, we only want proper users to have access to this system so the client's data is protected.

The next policy is 'Deny logon locally' and its template setting is 'Guests'. This setting restricts all members of the Guests groups from logging on to the system locally. This is extremely important to this environment. When this server is deployed we want all access to the system restricted to over the network. This prevents users from logging into the server and changing their passwords, it also further reduced the chance an intruder gaining access to system directly.

The next policy is 'Force shutdown from a remote system' and its template setting is 'Administrators'. This setting allows only Administrators to shut down the system from a remote location on the network. This is not very relevant to the mobile LAN environment.

The next policy is 'Increase quotas' and its template setting is 'Administrators'. This setting allows only Administrators to increase drive space quotas (if enabled). This setting is not relevant because quotas are not being used.

The next policy is 'Load and unload device drivers' and its template setting is 'Administrators'. This setting allows only Administrators to load and unload device drivers. This prevents users from changing system configurations and changing hardware on the system. This is another policy that is very important to the server. Since one of the main roles of the system is that of print server the proper drives for the printer must be loaded. By restricting this setting other users can't change the print driver which could cause delays for the team.

The next policy is 'Log on locally' and its template setting is 'Administrators'. This setting restricts the ability to log on locally to only members of the Administrators group. This setting along with the 'Deny logon locally' policy discussed above provides full control over which users can log on locally. By combining who can and who can't log on, the policies cover every contingency.

The next policy is 'Manage auditing and security log' and its template setting is 'Administrators'. This setting allows only Administrators the ability to change auditing settings on files, the registry, and Active Directory objects. Since the logs play an important part in managing a system you only want Administrators to

be able to change these settings. This policy is of low relevance is our environment since logs are used more for historical purposes than active monitoring.

The next policy is 'Restore files and directories' and its template setting is 'Administrators'. This setting only allows Administrators the ability to restore files and directories from a backup while bypassing specific file and directory permissions. This policy is low in relevance since no restoration of files and directories will take place on these systems.

The next policy is 'Shut down the system' and its template setting is 'Administrators'. This setting only allows Administrators to shut down the system. This prevents unauthorized parties from bringing down critical servers. However, in our environment the team might need to shut down the server to remove it from the client site for a weekend or maybe just nightly to further enhance security.

The last policy for this section is 'Take ownership of files and other objects' and its template setting is 'Administrators'. This setting only allows Administrators to change the ownership of the files and directories from a user to the Administrator's account. This is relevant to our environment because we don't want users taking control of other user's files. By taking control they can alter permissions and even delete the file.

The next section of Local Policies, Security Options, has a number of policies that are important to the mobile LAN environment. Below the settings are explained in more detail.

The first policy is 'Additional restrictions for anonymous connections' and its template setting is 'No access without explicit anonymous permissions'. This setting restricts the use of anonymous connections to the server. Now explicit permissions must be granted for an anonymous connection to be granted. This prevents other individuals (i.e. employees of the client) from plugging into the mobile LAN's hub/switch and getting access to this system.

The next policy is 'Allow system to be shut down without having to log on' and its template setting is 'Disabled'. This setting further prevents non-Administrators from shutting down the system. For our environment this setting is important, as stated above, the system may need to be moved frequently which would require shutting it down.

The next policy is 'Allowed to eject removable NTFS media' and its template setting is 'Administrators'. This setting is primarily for backup media, but restricts all NTFS media from being ejected unless using an Administrator account. This setting is not relevant to this environment.

The next policy is ‘Amount of idle time required before disconnecting session’ and its template setting is ’30 minutes’. This setting closes connections after 30 minutes of inactivity. This is important for the mobile LAN server because this helps mitigate the chance an authorized user who is connected walks away from their system allowing an intruder to directly access the system.

The next policy is ‘Automatically log off users when logon time expires’ and its template setting is ‘Enabled’. This setting will automatically log off a user when the user’s logon time passes (requires logon time to be configured for the user). This is not relevant to our environment because users are not logging into this server, they are only connecting to the shared folder and printer.

The next policy is ‘Do not display last user name in logon screen’ and its template setting is ‘Enabled’. This setting provides additional security by hiding the previous user logged on locally to the system. If this information is displayed an intruder already knows a very important piece of information, a valid system user account name. This setting has little relevance in this environment.

The next policy is ‘Prevent users from installing printer drivers’ and its template setting is ‘Enabled’. This setting restricts users from installing print drivers on the server. This is another policy that is extremely important in the mobile LAN environment. Since one of the main roles is that of print server you don’t want users to be able to install print drivers that might conflict with the default setup.

The next policy is ‘Prompt user to change password before expiration’ and its template setting is ’14 days’. This setting causes a reminder to be generated, starting 14 days before the user’s password expires and continuing until the user changes the password, requesting the user change their password. This is another setting with no relevance to this environment.

The final policy in this section is ‘Recovery Console: Allow automatic administrative logon’ and its template setting is ‘Disabled’. This prevents the systems from automatically logging into the Administrator account when the recovery console is run. This is important to our system since we don’t want any one to have access to the system locally. If the Recovery Console is started we don’t want the system to automatically log in with Administrative rights. This could allow unauthorized access.

Event Log

This section describes the settings for the event log. All of these settings provide standard security that is applicable to our environment. As stated above the logs are mainly for historical record instead of active monitoring.

Event Log Policy	Computer Setting	Explanation
Maximum application log size	81920 kilobytes	This sets the maximum size of the application log file.
Maximum security log size	81920 kilobytes	This sets the maximum size of the security log file.
Maximum system log size	81920 kilobytes	This sets the maximum size of the system log file.
Restrict guest access to application log	Enabled	This setting restricts a guest user's access to the application log.
Restrict guest access to security log	Enabled	This setting restricts a guest user's access to the security log.
Restrict guest access to system log	Enabled	This setting restricts a guest user's access to the system log.

System Services

This section describes the settings for the system services. Specifically these settings determine how a service is configured on startup and who has permission to change the services' settings. For the mobile LAN server these settings are very important. Since the servers role is so specific most services will not be used and if they aren't used then disabling them provides better security. None of the services listed below are required by system.

Service Name	Startup	Permission
Alerter	Disabled	Administrator: Full Control System: Read & Stop, Start and Pause Everyone: Read
ClipBook	Disabled	Administrator: Full Control System: Read & Stop, Start and Pause Everyone: Read
Computer Browser	Disabled	Administrator: Full Control System: Read & Stop, Start and Pause Everyone: Read
Fax Service	Disabled	Administrator: Full Control System: Read & Stop, Start and Pause Everyone: Read

Service Name	Startup	Permission
IISADMIN	Disabled	Administrator: Full Control System: Read & Stop, Start and Pause Everyone: Read
Internet Connection Sharing	Disabled	Administrator: Full Control System: Read & Stop, Start and Pause Everyone: Read
Messenger	Disabled	Administrator: Full Control System: Read & Stop, Start and Pause Everyone: Read
MSFTPSVC	Disabled	Administrator: Full Control System: Read & Stop, Start and Pause Everyone: Read
NetMeeting Remote Desktop Sharing	Disabled	Administrator: Full Control System: Read & Stop, Start and Pause Everyone: Read
Remote Registry Service	Disabled	Administrator: Full Control System: Read & Stop, Start and Pause Everyone: Read
Routing and Remote Access	Disabled	Administrator: Full Control System: Read & Stop, Start and Pause Everyone: Read
SMTPSVC	Disabled	Administrator: Full Control System: Read & Stop, Start and Pause Everyone: Read
SNMP	Disabled	Administrator: Full Control System: Read & Stop, Start and Pause Everyone: Read
SNMPTRAP	Disabled	Administrator: Full Control System: Read & Stop, Start and Pause Everyone: Read
Telnet	Disabled	Administrator: Full Control System: Read & Stop, Start and Pause Everyone: Read

Service Name	Startup	Permission
W3SVC	Disabled	Administrator: Full Control System: Read & Stop, Start and Pause Everyone: Read

File System

This section describes the settings for the file system, such as specific permissions for files and directories. Only select file system permissions from the template are listed below. All of these permissions are relevant to the mobile LAN server because we want to restrict as much access to system files and directories as possible. These files and directories are extremely important to all windows systems.

Object Name	Permission
%ProgramFiles%	Administrators: Full System: Full Creator Owner: Full Users: Read and Execute, List
%SystemDrive%\autoexec.bat	Administrators: Full System: Full
%SystemDrive%\boot.ini	Administrators: Full System: Full
%SystemDrive%\config.sys	Administrators: Full System: Full Users: Read and Execute, List
%SystemDrive%\Documents and Settings\Administrator	Administrators: Full System: Full
%SystemDrive%\IO.SYS	Administrators: Full System: Full Users: Read and Execute, List
%SystemDrive%\MSDOS.SYS	Administrators: Full System: Full Users: Read and Execute, List
%SystemDrive%\ntbootdd.sys	Administrators: Full System: Full
%SystemDrive%\ntdetect.com	Administrators: Full System: Full
%SystemDrive%\ntldr	Administrators: Full System: Full
%SystemDrive%\Program Files\Resource Kit	Administrators: Full System: Full

Object Name	Permission
%SystemDrive%\Temp	Administrators: Full System: Full Creator Owner: Full Users: Traverse Folders/Execute Files, Create Files/Write Data, Create Folder/Append Data (Subfolders and files only)
%SystemRoot%	Administrators: Full System: Full Users: Read and Execute, List
%SystemRoot%\$NtServicePackUninstall$	Administrators: Full System: Full
%SystemRoot%\CSC	Administrators: Full System: Full
%SystemRoot%\regedit.exe	Administrators: Full System: Full
%SystemRoot%\repair	Administrators: Full System: Full
%SystemRoot%\security	Administrators: Full System: Full Creator Owner: Full
%SystemRoot%\system32	Administrators: Full System: Full Creator Owner: Full Users: Read and Execute, List
%SystemRoot%\system32\config	Administrators: Full System: Full
%SystemRoot%\system32\dllcache	Administrators: Full System: Full Creator Owner: Full
%SystemRoot%\system32\DTCLog	Administrators: Full System: Full Creator Owner: Full Users: Read and Execute, List
%SystemRoot%\system32\ias	Administrators: Full System: Full Creator Owner: Full
%SystemRoot%\system32\Ntbackup.exe	Administrators: Full System: Full
%SystemRoot%\system32\rcp.exe	Administrators: Full System: Full
%SystemRoot%\system32\regedt32.exe	Administrators: Full System: Full

Object Name	Permission
%SystemRoot%\system32\rexec.exe	Administrators: Full System: Full
%SystemRoot%\system32\rsh.exe	Administrators: Full System: Full
%SystemRoot%\system32\secedit.exe	Administrators: Full System: Full
%SystemRoot%\system32\spool\printers	Administrators: Full System: Full Creator Owner: Full Users: Traverse Folder, Execute File, Read, Read Extended Attributes, Create folders, Append Data
%SystemRoot%\Tasks	Administrators: Full System: Full Creator Owner: Full
%SystemRoot%\Temp	Administrators: Full System: Full Creator Owner: Full Users: Traverse Folders/Execute Files, Create Files/Write Data, Create Folder/Append Data (Subfolders and files only)
c:\autoexec.bat	Administrators: Full System: Full
c:\boot.ini	Administrators: Full System: Full
c:\config.sys	Administrators: Full System: Full
c:\ntbootdd.sys	Administrators: Full System: Full
c:\ntdetect.com	Administrators: Full System: Full
c:\ntldr	Administrators: Full System: Full

Applying the Template

Before we apply the security template to the server the system should be backed up. The standard way to store this backup copy is to create an image of the hard drive using Norton Ghost. This way if after the application of the template the system is inoperable you can use the backup image file to quickly recreate the system. Then you can fix the template and apply it again. Once you have

successfully applied and tested the template a final ghost image can be created for future deployments and the temporary backup image can be deleted.

The following steps were preformed to apply the template to the system:

1. Log in locally to the system using the Administrator account.
2. Start the Microsoft Management Console (MMC) by clicking **Start**, **Run…** and typing "mmc", then click **OK**.
3. After the MMC windows opens go to the **Console** menu.
4. Under the **Console** menu choose **Add/Remove Snap-in…**
5. Next, click the **Add...** button.
6. From the Add Standalone Snap-in box choose **Security Configuration and Analysis**, then click the **Add** button, followed by the **Close** button.
7. Now click the **OK** button to close the Add/Remove Snap-in window
8. Next, save the console by choosing **Save** under the **Console** menu.
9. Choose a location for the console and a name for the file. (For example save the file as Security.msc on your Desktop)
10. Close the MMC.

This created an easy way to access the Security Configuration and Analysis snap-in. For future changes to the security policy this can be used. The MMC can also be used to manage other system settings like Users & Groups, etc. Now, continuing with the process:

11. Open the console you just created.
12. Right click on Security Configuration and Analysis in the left side pane.
13. Choose **Open Database…** from the context menu.
14. Now create a new database file by typing a name in the File name field and clicking Open.
15. Next you are asked to choose a template file to use. Browse to the Win2kSrvGold_R1.0.inf, select it and click the **Open** button.

If you want to compare the computer's current settings to those in the security template follow the steps below. This is not necessary in this case (for the mobile LAN server) because the template is definitely going to be applied.

16. Right click on Security Configuration and Analysis again and choose Analyze Computer Now… (This will compare the computer's current settings to those in the security template)
17. Select a location for the log file and click **OK**.
18. Review the log file

To finally apply the template follow, these steps:

19. Right click on Security Configuration and Analysis again and choose **Configure Computer Now…**
20. Select a location for the log file and click **OK**.
21. The application is complete; all of the settings take place immediately.

Over time, as more security flaws are discovered in Windows the settings in the template will updated meaning in turn that systems must also be updated. The best long-term solution to this problem is the implementation of Microsoft Active Directory and Group Policy. More information on this topic is covered in the Evaluation section later in the document.

Testing the Template

After the template is applied to the system one set of tests was preformed on the system to verify the settings in the template were applied as expected. A second set of tests was preformed to make sure the system is still functioning correctly after the template was applied.

The security settings tests served only as sample of the overall templates effectiveness since testing every single setting in the template would require extraordinary time and effort. The tests were:

1. An administrator's attempt to change a user's password to a password that doesn't meet the complexity policies implemented
2. A remote user's attempt to create subfolders and files under the shared data folder
3. A user's attempt to logon to the system locally

Settings Test 1

The first test conducted was designed to test the password policies implemented by with the template. This test was selected since good password policies are vital to the security of any system, especially one that is storing confidential data.

First a user, 'jsmith', was created on the system by the Administrator (as described above in the Software Setup section). This user's password was set to 'password'. After the security template was implemented a password change was attempted by the Administrator using 'mydog' as the new password. The expected result should be the system rejecting the password since it doesn't meet length or complexity standards. Sure enough the attempt to change the password resulted in the following error message being displayed (Figure 2).

Figure 2

Now in actuality the Administrator would probably be aware of the password complexity rules in place and would not try to change the password to 'mydog'. However, if the setup of users was handled by a temporary worker or by a new member of the technical support staff this policy will prevent simple passwords form being used.

Settings Test 2

The second test of the server's settings was the permissions test. Using a client workstation laptop with the user account 'test' currently logged in, an attempt was made to connect to the mobile LAN server over the network. The server requested a username and password for the connection (Figure 3). Based on the templates security policies only members of the Administrators and Users groups should be able to log in using both a correct user name and password. If the correct combination of user name and password are not entered the expected result would be a failure to connect to the mobile LAN server and a number of events logged in the event log for each failed attempt to connect.

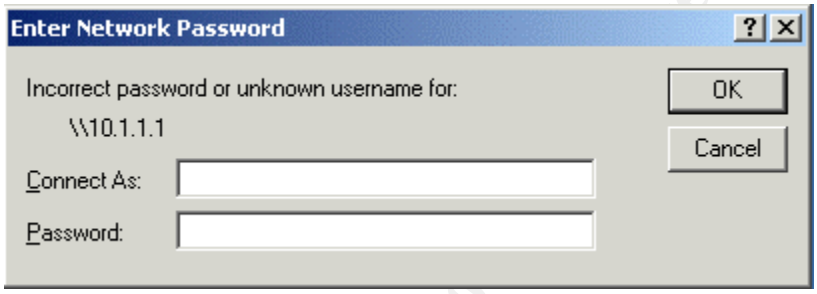

Figure 3

A number of entries for the user name and password were tried, such as Administrator with no password, Guest with no password, no username or password, etc. However, no combination would work. After reviewing the Security Event Log on the server the failed attempts were visible. One such failure is shown below (Figure 4). Again, since the logs are not being actively monitored this test is designed more to ensure proper logging is occurring than to alert the administrator of a possible attempt to compromise the system.

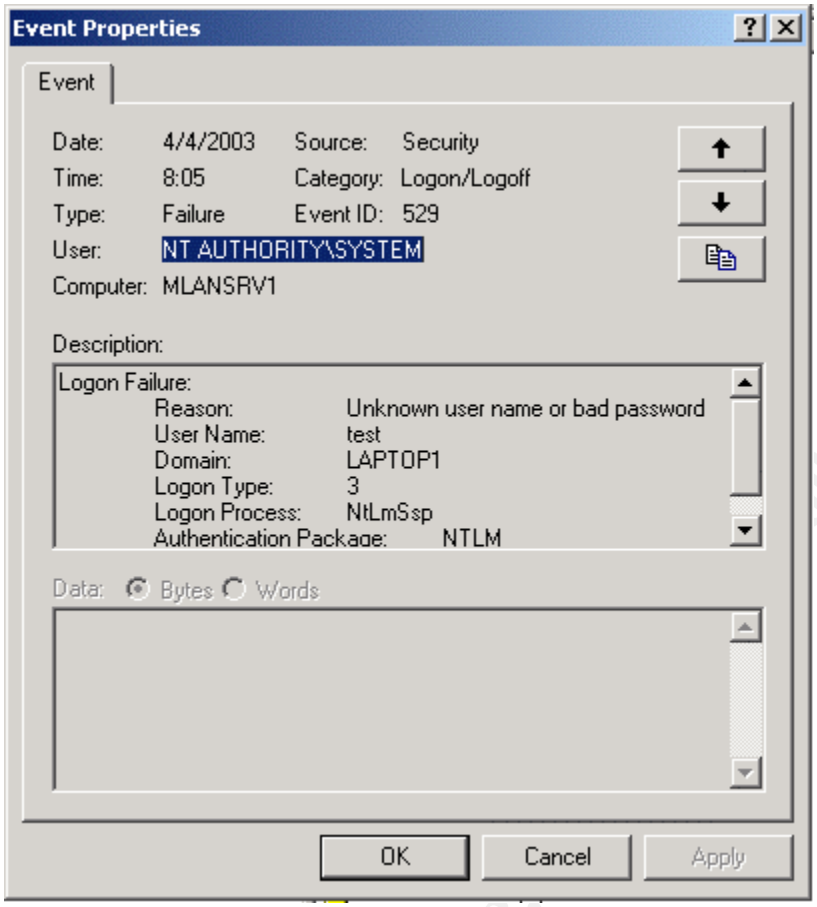

Figure 4

Settings Test 3

The final test conducted was designed to test the setting for allowing local logons to the server. This is important for the mobile LAN server because users should not be using the system for anything other than the roles mentioned previously. To test this policy an attempt to logon locally using the 'mcullen' account was made. The expected result was an error message and a failure entry in the security event log. The test resulted in the following error message:

```
The local policy of this system does not permit you to
logon interactively.
```

Also, as expected the following entry (Figure 5) was recorded in the security event log.

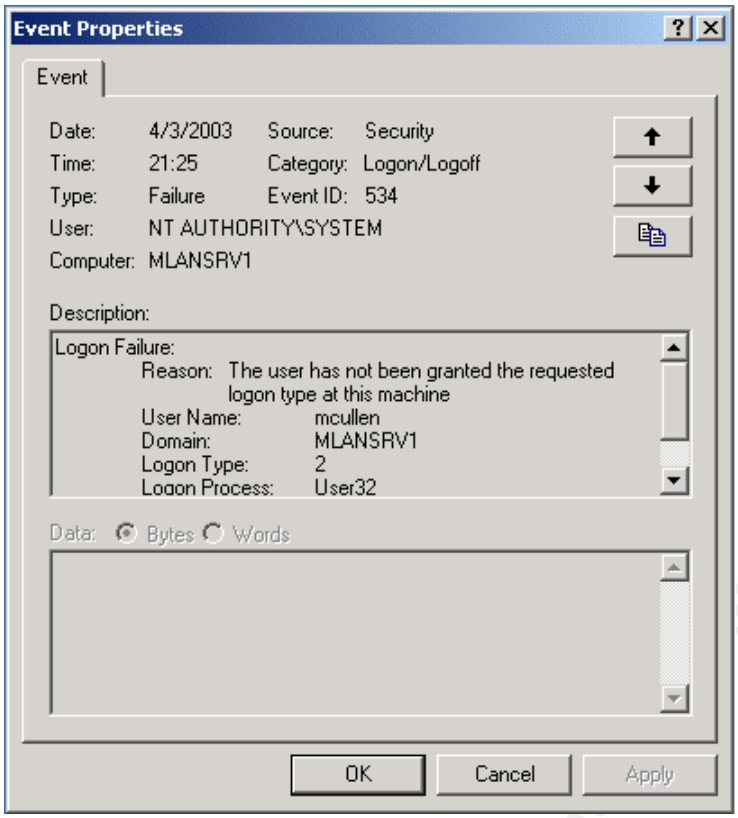

Figure 5

Functionality Test 1

The first functional test of the mobile LAN server dealt with the assignment of DHCP addresses. The system is setup to serve a DHCP address to any computer connecting to the network. We will test this functionality by physically connecting a workstation to the network by plugging into the mobile LAN hub/switch. The mobile LAN server has a DHCP server running with a scope of 10.1.1.2 to 10.1.1.16 and no reserved addresses. The expected result for this test was a successful connection and IP address assignment in the range stated above (with the exception of 10.1.1.1 since this address is currently assigned to the server itself). After plugging in the workstation a command prompt window was opened. The 'ipconfig' command (Figure 6) was run resulting in the workstation reporting it was assigned the IP address 10.1.1.2 as expected.

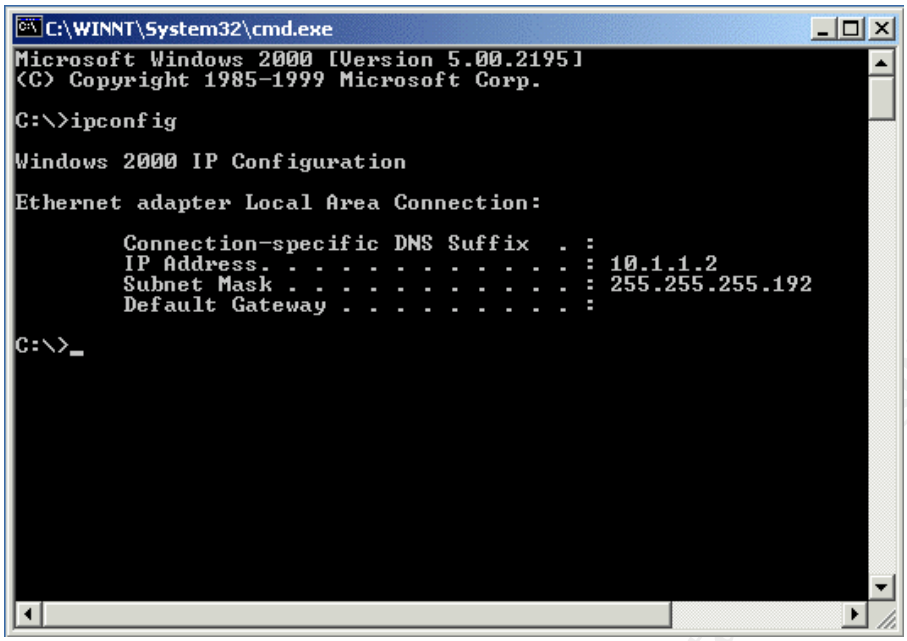

Figure 6

Functionality Test 2

Another role of the mobile LAN server is printer sharing. The second test was an attempt to connect to the shared printer and print a document. The printer is being shared as 'Printer'. No problems or anomalies were anticipated. Using another workstation laptop a connection to the server was attempted by entering '\\10.1.1.1' in the Start – Run… dialog box. The 'Enter Network Password' dialog (Figure 7) appears. For the user name, 'mcullen' was used and the appropriate password was also entered.

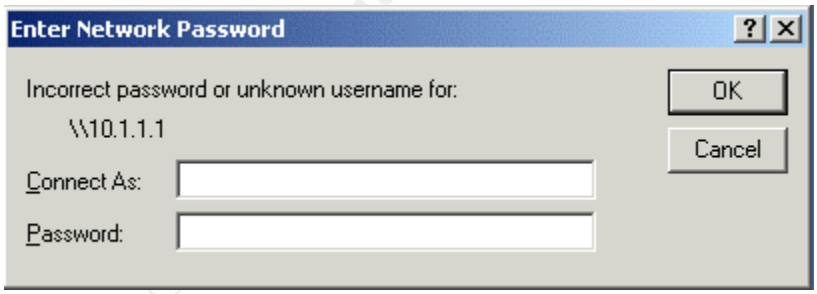

Figure 7

Then a window appeared showing all of the resources currently being shared by the mobile LAN server. To connect to the printer (Shared as 'Printer') you right click on the printer icon and choose 'Connect…'. A warning window appears asking if you want to install the proper printer drivers from the server. After clicking 'Yes', the printer is installed. Next, Microsoft Word was started and a test document was opened. To print the document, choose 'Print…' from the 'File'

menu. At the top of the 'Print' dialog box choose the mobile LAN printer from the drop down menu, and then click the 'Print' button. The document printed without any problems.

Functionality Test 3

The next test was designed to ensure the File System permission policies in the template did not affect the server's shared data folder. Based on the security template system users should have the ability to manipulate folder and create files in the shared data directory. First using a workstation laptop, the user 'bjohnson' connected remotely (over the network) to the shared folder 'LAN Storage'. After a successful connection to the folder the user attempted to create a subfolder named 'Client Contacts'. The folder was created with no problems. The Access Control Settings for Client Contacts (Figure 8) show that Betsy Johnson (username: bjohnson) was the owner of that folder.

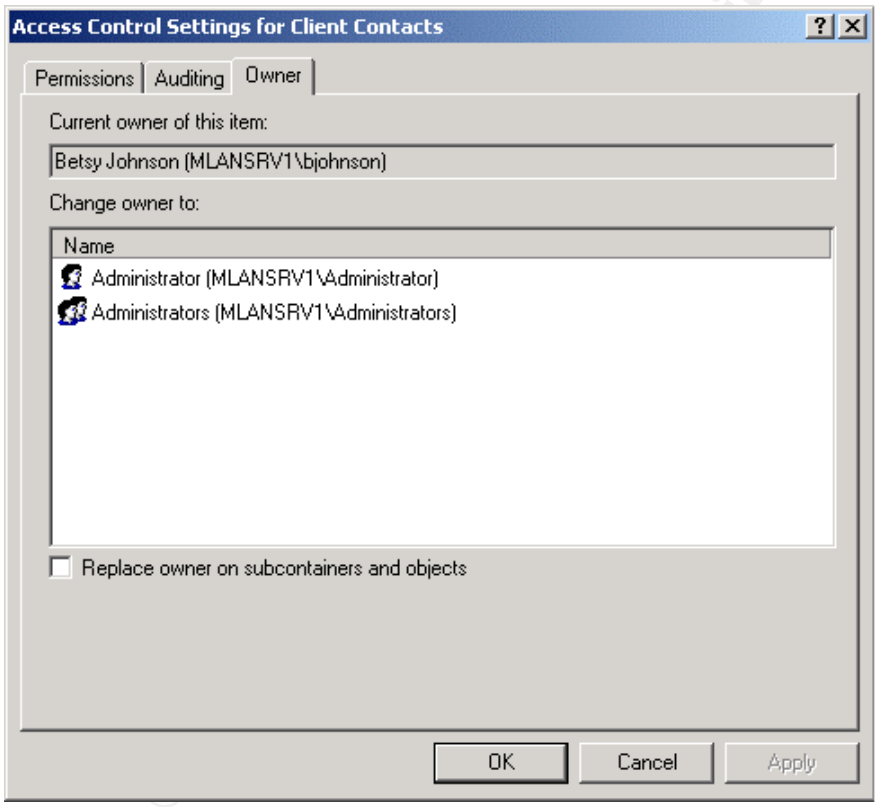

Figure 8

Evaluating the Template

Based on the research and testing done over the course of this assignment the following areas were evaluated.

- Were the templates security settings inappropriate (i.e. too strong, too weak)?
- What changes should be made to the template for more general use?
- What changes should be made to the template for the mobile LAN environment?
- How did the template affect the system and application operation?
- What further research could be done on security templates?
- Are there more efficient methods for updating, managing these systems?

Template Appropriateness

While researching the CIS template, the information provided, along with the template's own settings, seemed very appropriate for the mobile LAN. First, the template is not for use on domain controllers (DC) and since the system is not functioning as DC it met the needs. Secondly the server is not connected to the Internet or functioning as a web server, so a template that configured Microsoft Internet Information Server or another web server would not have been necessary. Lastly the CIS designed this template to be comprehensive and incorporate the recommendations of many organizations. This level of detail provides very good security without a large amount of manual configuration.

Specifically a number of settings were really not appropriate for the mobile LAN environment. First the 'Enforce password history' policy and its template setting of '24 passwords remembered' is overkill. In this environment the length of the mobile LAN deployment is rarely longer than 60 days, so this policy combined with the 90 day password age setting means a 24 password history is unnecessary. This policy should be removed from the template.

The second policy that is not appropriate for this environment is 'Deny logon locally'. The template has the setting of 'Guests'. This setting restricts all members of the Guests groups from logging on to the system locally. For the mobile LAN we also want to restrict the Users group, since this is the group that contains all of the accountants on the engagement team.

The third policy that is requires changing to make it more appropriate is 'Shut down the system' and its template setting of 'Administrators'. This setting only allows Administrators to shut down the system. This prevents unauthorized parties from bringing down critical servers. However, in our environment the team might need to shut down the server to remove it from the client site for a weekend or maybe just nightly to further enhance security. So the proper change for this setting would be to include the Users group along with Administrators as the groups that have access to shut down the system. The fourth policy 'Allow system to be shut down without having to log on', and its template setting of 'Disabled' goes along with the previous policy. In this environment the team needs to be able to shut the server down without logging

in locally, for one because they can't log in locally due to another policy in the template and secondly there is no need to log in just to shut down.

The final policy whose setting is not appropriate is 'Prompt user to change password before expiration'. With a setting of '14 days' this policy means nothing to this environment. Since users aren't logging in to the server they will never receive this message. Also, as stated above chances are slim that team will even be using the server when this message appears since the jobs only last 60 days.

Finally a number of other policies in the template are very appropriate to the environment. All of the policies in the System Services and File System sections are appropriate for this environment. All non-essential services are disabled within the template and because of the basic nature of the server this causes no disruptions to the functionality. The File System section is made up policies that assign permissions for important system files and directories. All of these permissions are appropriate and help secure the system.

Changes to the Template

The template is very good for the general security of a non-domain controller Windows 2000 server. As noted previously the template is not designed for use on a DC. The template covers all areas for the security policies for a Windows 2000 machine adequately so there are no general changes to make to the template. However, for the mobile LAN environment a number of more specific changes could be made to improve security. First, by enhancing the file system permission settings you could have better control over which users can manage files and folders. As it stands now any authorized user can create files and folders in the shared folder. But, another authorized user can delete, move, or change those files and folders, whether it be on purpose or by accident. This could cause major problems with client data and work products. Another recommended change was the creation of a mobile LAN Administrator account that would have the ability to manage the files and folders in only the shared data directory, as well as other day to day operations. This would make it easier to enhance and maintain security since this mobile LAN Administrator would be on site with the project team. A change like this would require changes to the template so this administrator account could have some of the system administrator's rights and privileges.

Effects of the Template

Since the role of the mobile LAN server is limited and very specific the effect of the template on the system was very minimal. The research conducted prior to the selection of the CIS template proved valuable during the testing phase. Each of the six tests conducted on the system after the template application resulted in the anticipated and proper outcomes. None of the three system settings tests or

the three functionality tests resulted in errors or adverse system operations. If this had been a more complex server, for example one that was connected to the Internet and was hosting a web site, then more anomalies would have been experienced. Also, since the testing was limited to just six tasks, problems could be found later on when the system is used more frequently.

Further Research

There remain a few areas where more research could be done on securing a Windows 2000 Server, specifically more research on mobile LAN configurations and setups. Although no information was found when researching templates, a more thorough search of the World Wide Web, as well as published resources could yield specific information on securing a file and print server with DHCP addressing. This research could yield much more detailed risks faced by such a system along with security settings/policies that would be more appropriate.

As far as more research on general Windows 2000 Server security templates, the major organizations that publish this information were explored. These organizations included the NSA, Microsoft, CIS, SANS, Defense Information Systems Agency, and the National Institute of Standards and Technology. More specific information about securing different applications and services that run on the Windows 2000 Server platform can most likely be found, however, that was not relevant to this mobile LAN server.

Managing the Template

The management of security policies within Windows has been a challenge since the advent of the operating system. Windows 2000 has made the biggest strides in making the application, updating, and management of security policies more efficient. Although the template for the mobile LAN server was only applied on the local system with a somewhat manual process, the process itself was fairly easy. Use of the Security Configuration and Analysis snap-in for the MMC is great for a small number of systems. However, most organizations are supporting many users with multiple servers, each conducting multiple processes or functions.

A more advanced and manageable solution for a large organization deploying multiple mobile LANs would utilize Active Directory and Group Policy. If the organization is not already using it, the first step for this type of deployment would be to have Active Directory implemented throughout the network environment. Although you can still achieve a certain level of automation and centralized management without Active Directory, with it network management would be much easier and efficient. However, the cost of implementing an entire Windows Active Directory network is substantial.

If Active Directory is in use the next steps are straightforward. To enhance security and allow for future server functions (i.e. remote connectivity, domain replication) each of these servers could be configured as backup domain controllers (BDC). As BDCs the domain's security settings could easily be passed along to the mobile LAN servers. Also, if Internet connectivity was needed the mobile LAN server functioning as a BDC could have direct contact to the organizations network through a virtual private network. This would provide a mechanism for remote administration and more frequent updating.

Next, a specific organizational unit (OU) would be created for the mobile LAN servers. This OU would allow the domain administrator to configure all of the appropriate settings and updates from one central location. Using Group Policy the administrator can push out the settings to all of the mobile LAN servers. Then when updates are required the administrator can easily make the changes once instead of changing the settings of each server manually at the machine itself. The use of a specific OU for just the mobile LAN servers makes all administration tasks easier and more efficient, not just security. Using Group Policy and scripting a number of different types of updates can be rolled out to all servers, for example, making sure each machine has the latest printer drivers.

In the case of this accounting firm, the use of the stand alone server was more appropriate since the Active Directory infrastructure was not already in place. Not only that, but the network environment is NetWare so adding a Windows domain to an environment would create more issues. Making the mobile LAN server is a slight possibility, however, with more and more companies moving to Active Directory this type of investment would not pay off in the long term.

Conclusion

The use of a security template to secure Windows 2000 Server is very helpful in improving security throughout an organization's network. It allows organizations, without the time or resources to design a custom solution, to implement good security measures easily. However, proper research and understanding of the templates and the settings contained within them is vital to really improving and maintaining a secure network environment. Also, proper testing must be conducted on the template before all settings are deployed in the environment. This may lead to slight modification in the template to better suit the needs of the organization. Finally, to maintain a high level of security and efficient management the use of Active Directory and Group Policy is essential.

References

Shawgo, Jeff. "Windows 2000 Server Operating System Level 2 Benchmark Consensus Baseline Security Settings." Version 1.0. January 1, 2003. URL:https://www.cisecurity.org/tools2/win2000/W2K-Srv.pdf

Fossen, Jason. "Windows 2000/XP Active Directory". Version 1.0. August 12, 2002. SANS Institute

"Microsoft Baseline Security Analyzer (MBSA) Version 1.1 Q&A". Microsoft Technet. January 9, 2003. URL:http://www.microsoft.com/technet/security/tools/Tools/mbsaqa.asp

"Windows 2000 Server Baseline Security Checklist". Microsoft TechNet. 2001. URL:http://www.microsoft.com/technet/security/tools/chklist/w2ksvrcl.asp

"Microsoft Network Security Hotfix Checker". Microsoft. February 18, 2003. URL:http://support.microsoft.com/default.aspx?scid=kb;en-us;303215&sd=tech

Fossen, Jason. "Windows 2000/XP Group Policy and DNS". Version 1.0. August 6, 2002. SANS Institute

Bartock, Paul F. "Microsoft Windows 2000 Network Architecture Guide". Version 1.0. April 19, 2001. National Security Agency

Last Updated: May 23rd, 2017

Upcoming Training

SANS Cyber Defence Canberra 2017	**Canberra, Australia**	**Jun 26, 2017 - Jul 08, 2017**	**Live Event**
SANSFIRE 2017	**Washington, DC**	**Jul 22, 2017 - Jul 29, 2017**	**Live Event**
SANS Virginia Beach 2017	**Virginia Beach, VA**	**Aug 21, 2017 - Sep 01, 2017**	**Live Event**
SANS Network Security 2017	**Las Vegas, NV**	**Sep 10, 2017 - Sep 17, 2017**	**Live Event**
SANS vLive - SEC505: Securing Windows and PowerShell Automation	**SEC505 - 201709,**	**Sep 18, 2017 - Nov 06, 2017**	**vLive**
Secure DevOps Summit & Training	**Denver, CO**	**Oct 10, 2017 - Oct 17, 2017**	**Live Event**
SANS San Francisco Winter 2017	**San Francisco, CA**	**Nov 27, 2017 - Dec 02, 2017**	**Live Event**
San Francisco Winter 2017 - SEC505: Securing Windows and PowerShell Automation	**San Francisco, CA**	**Nov 27, 2017 - Dec 02, 2017**	**vLive**
SANS OnDemand	**Online**	**Anytime**	**Self Paced**
SANS SelfStudy	**Books & MP3s Only**	**Anytime**	**Self Paced**