Global Information Assurance Certification Paper

With a Kiosk, How Secure is Secure?

Securing Windows
GCNT Practical Assignment
Version 3.0 – Option 2
August 13, 2001

Table of Contents

Securing a Windows 2000 Kiosk

Introduction

The original idea of this project was to create a computer image that could be used at multiple locations throughout the organization. This system would be used to access a community web server to print out the user's personal data on a locally attached printer. This would allow the user to printout data locally without having to rush to the network printer to keep nosy people from reading personal financial information. The catch to this project was that anybody had to be able to log into this system. This included people from affiliated companies that did not have company network access, but were allowed in certain public access areas of the buildings. This meant that the system could have no access to the corporate servers, and needed as little maintenance as possible.

Developing a secure image sounded like an interesting assignment, so I volunteered for the mission. I began working away armed with ideas and knowledge from TechNet, Microsoft training, some security books and personal experience. My knowledge from previous work with Windows NT 4.0 started to lead towards security registry pokes, but I decided to opt to use the Windows 2000 security templates and related tools provided in the Microsoft operating system. These tools would make it much easier to secure the system.

Specifications

The computer system specifications will be a little different everywhere because each site purchases their own computer systems. It would be nice if everybody had the exact system, but sometimes that is not possible. The system will also be running on one of the older computers that were left over after the last sweep of system upgrades. Since there will not be any need for great horsepower, the older hardware platform will work without any problems. The older hardware had also been running Windows 2000, so compatibility issues will not be a major problem. As far as the image we will be developing, this is one of the reasons Windows 2000 was chosen over Windows NT. Windows 2000 is much more forgiving with different hardware configurations because of the "plug and play" ability. Plug and play is not perfect, but it is not as temperamental to hardware configuration differences as Windows NT. Here are the general specifications for the class of systems to be used:

Brand:	varies
Processor:	Pentium III/667
Memory:	128MB (will have been upgraded from the original 64MB)
Hard drive:	10GB EIDE
CD-ROM:	32X IDE
Video:	2X or 4X AGP Video card (most likely ATI Rage IIC chipset)

Sound card:	None (has been removed)
Printer:	HP LaserJet III or IV series
Software:	Windows 2000 Professional
Applications:	Latest version of Internet Explorer (no other software packages will be installed or used this system)

Applications and the computer configuration

This system will only be used to access a community web server through HTTPS (port 443). The system will have no other function. This access will be performed using Internet Explorer. No extra plug-ins or ActiveX controls will be required. This will greatly simplify the software requirements and compatibility issues with the system.

Computer function and the level of security

The key to deciding what type of system this will be is the access level needed. If the company employees only accessed this system, it could be setup as a standard user workstation with individual logins using your network operating system of choice. The intended application of this system will be to allow anybody – including non-company employees – access to a community web server that is not located on the local network. To accomplish this, the system will require a generic logon with absolutely no access to the rest of the networking infrastructure except to the intended server. The most viable solution will be to setup this system as a kiosk. The function of a kiosk is a system that is publicly accessible and can be used by anyone (such as an ATM machine). This will be the role of the system.

Securing the kiosk using a security template

The default installation of Windows 2000 Professional does not have all the required lock downs needed for a kiosk. A standard install is great for other situations, but a kiosk must be as locked down as possible. To secure this system as much as possible, the Microsoft template with the highest amount of security will be applied and analyzed. This allows many security changes to be made at one time in one place. The template we will be using is called HISECWS.INF, and it is provided with the Windows 2000 operating system. This template will have to be modified for the security needed on the kiosk. The security template section of this document discusses the exact differences between the default Windows 2000 installation settings, the changes made by the HISECWS.INF template, and changes needed to the template for usage on the kiosk.

Access Accounts

Access into the kiosk must be secure for all users. No information must remain on the system after the user logs out. To accomplish this successfully, the kiosk login account will be a user account that is only a member of the "Guests" group. Using this member group, all login profile information will be deleted as soon as the user logs out. The question that should come to mind here is "Why not just rename the Guest account and use it to log into the system?". The main reason for

this is the operating system handling of the actual Guest account. This account is treated differently than a user that is a member of the Guests member group. The primary problem with the Guest account is the inability of scripts to run on login or logoff. Scripts work without any problems for users belonging only to the Guests member group.

User access and auditing

The most difficult management part of a kiosk is keeping track of what the user does. Every user logs into the machine with the same account, therefore there is no way to determine which user has performed what actions. Even though this is the case, full auditing must be enabled on this system. It would be a wise investment to get a cheap VCR and video camera to record the kiosk. If the system is in an area where this cannot be accomplished, then that risk will have to be taken into consideration before deciding to deploy these systems. Auditing will still help out in determining if problems came from that specific kiosk and is there a time correlation with the non-allowed action. The best setup would be to place this computer in a de-militarized zone (DMZ) that only has local network to external site access. Please keep this problem in mind when deploying kiosks!

Proposed Solution

All this leads us to our proposed solution. Here is a quick rundown on the specification requirements of the kiosk:

- There will be single image that will be deployed at multiple sites. Preferably, the image will be tolerant to changes in the hardware platform to allow the usage at different sites with the least number of problems.
- The system will only have two accessible accounts on it: one account will be for maintenance and the other for user access. The maintenance account will have administrative rights to keep the system updated, and the user account will have extremely limited access.
- The administrator account will be set to expire as per the company password policy.
- The user account will be setup as a guest account to guarantee that the data from the previous user will be totally removed from the system when the user logs off. This will allow for easier administration of the user login profile. The password will not be able to be changed by the user, and the password will be set to never expire. Because this system will be general access, there is not a need to be constantly changing the user account password.
- The only application used on this machine will be Internet Explorer.
- No network logon access will be allowed, except for access to the community web server. This server will only have access via secure socket layer (SSL) web access.
- No screen savers will be allowed to prevent the user from leaving the system unattended.
- A logon notice will be required.

- Full auditing will have to be enabled to determine what the user was doing, even though the account will be a generic account.
- The system will be updated via the administrative account on the system. It would be much easier to update the machines automatically, but this option is not available due to the placement of these kiosks.
- The machine will only be able to access a community web server over SSL that is not on the local company network.
- The local technician as required by the home office will update the system manually using an update CD-ROM sent to the local site as is needed.

Working with security templates, applying local group policies, and writing some custom programs will be used to attain the above results. Only the security template is documented in detail. At the end of this document, the user is pointed in the right direction as to what needs to be done to complete the creation of the kiosk.

Author's Note

Keep in mind that a kiosk can be implemented and secured in many different ways. This is just one method. These steps may or may not apply to how you would like to build this type of system. If you wish to actually build a kiosk, I would suggest thoroughly reading this document and then picking the changes that would apply to your specific needs. With all that said, let's begin!

Windows 2000 Software Installation on a Slicked Machine

We will begin our installation with the Windows 2000 CD in hand and one of the future kiosk computers installed with a slicked hard drive (no operating system, previous partitions, etc.). Since this system is not an ordinary workstation, the installation of Windows 2000 will be approached a little differently. The common software that is usually installed will be limited as much as possible. Remember that the only application we are concerned about is Internet Explorer.

First phase of the Windows 2000 installation

Begin the installation by booting the Windows 2000 CD or using boot disks (if needed). Even though it is practice for a highly secure system to have two partitions, this system has not been donned important enough to need this security measure. The same does not go for NTFS. NTFS is a must for this type of application so that we can lock the user out of as much of the system as possible. After the reboot, begin phase two of the Windows 2000 installation.

Second phase of the Windows 2000 installation

This is the phase where we start making some unique changes. To begin with, custom network settings will be used. The only network connectivity needed is simple TCP/IP; therefore "File and Printer Sharing for Microsoft Networks" and "Client for Microsoft Networks" should be uninstalled. Note that it should be UNINSTALLED and not just simply unchecked. This client could also be uninstalled after the software installation has been completed, but for this build we will go ahead and remove it in this phase of the Windows 2000 installation. Security templates work great, but they do not go as far as removing services. Why should these be removed? Here are the reasons:

File and Printer Sharing for Microsoft Networks

This option was created to allow sharing of resources to other users on the network. The kiosk will most definitely not be used for this purpose. When installed, this option installs two services: Browser service and Server service.

The Browser Service

These will not be needed for this kiosk installation. The kiosk should be involved with the rest of the network as little as possible. Having the browser server installed and enabled would allow the kiosk to function as a master browser (contain a list of all the machines on the network) or become a backup browser. This will also remove a little network traffic when the system boots up created by the kiosk broadcasting to find the master browser and then querying to be a possible backup browser.

The Server Service

This service is one of the most dangerous of all the Microsoft services. If a system is setup right out of the box with a known administrative account and weak password, consider this system hacked. It takes very few steps to

completely own the system if it can be connected to remotely using the IPC$ share. The deletion of the hidden drives (C$, D$, etc.) only provides a limited amount of security because a user with an IPC$ connection can add them right back in. The last thing you would want is the kiosk to be compromised and loaded with a key capture program that would conveniently send out the usernames and passwords entered by the users accessing their personal financial data. As the saying goes, the system is only as strong as its weakest link: ALWAYS USE STRONG PASSWORDS.

Client for Microsoft Networks

The reason this is removed is because the client is unnecessary for the setup of this kiosk. The client itself contains the workstation service and messenger service.

The Workstation Service

In most environments, the workstation service is not a problem and is also required in Microsoft networks for all server access authentications. This service causes a small amount of network broadcast traffic if using NetBIOS for connections (a lot more traffic if the workstation is not pointing at a WINS server), but is otherwise fairly quite. So why would you want to disable it? Only install the bare minimum needed to access what needs to be accessed. We will be accessing a community web server through https. This access will not require any RPC connections; therefore there will be no Microsoft authentication except through the web browser. The web browser access will authenticate through the destination web server over SSL.

The Messenger Service

This falls under the same category as the workstation service. If it is not essential for the operation of the kiosk, do not install it. The user at the kiosk will definitely not need to send out messages to other users and workstations. This could also create problems with user spoofing. The rogue user could start a conversation with someone on the network and emulate someone else through information gathered through social engineering. No one would ever send a password to a user simply based on a Microsoft message, right?

Third phase of the Windows 2000 installation

When prompted with the "Network Identification Wizard" page, make sure to check "Users must enter a username and password…". Now, before you stop reading right here and say "…but the idea of a kiosk is a system that auto logs in and never needs a password", listen to the explanation. If this system was on its own network and never set up for auditing to fend for itself, this would not be a problem. However, there is one crucial point missing here: legalities. If you audit what the user is doing nowadays, the user must know ahead of time if this is being done. The user has to be able to choose whether to use the system and consent to

monitoring, or go elsewhere. If this banner was not on the system, it would create problems in the court system when the user simply says "I never agreed to be monitored!". You cannot legally tap a phone line without the appropriate approvals, and the same goes for tapping into the system and network activities. In the last few years, this has become even more of an issue with the increasing thorough ability of security software and hardware. The generic username and password can even be posted using a sticky on the monitor, as long as the user is required to click "OK" on the logon banner before logging into the system. This system will also be deployed in a company building where it never hurts to have something that makes hackers think twice before proceeding.

Updating the Windows 2000 Workstation

Now that the basic Windows 2000 software has been installed, there are a few more things to complete before working with the security template. The system must first be brought up to date on all relative security patches and drivers.

Installation of Windows 2000 drivers

Only install the necessary Windows 2000 (and non-Windows 2000) hardware device drivers. As tempting as it may be, users really do not need the latest 3D accelerator video drivers to surf the community web server. If a Windows 2000 driver is available, use it. The same goes for the sound drivers; do not install them if the pages the user accesses will never have any sound. This will make life a little easier when trying to diagnose problems on different hardware platforms. Last of all, there should NOT be a modem installed in this machine. If there is a modem in the system, remove it immediately and install it in another machine where it can be properly utilized.

Installation of Windows 2000 service pack 2 (SP2)

As everybody in security knows, the first few steps of any build process is to patch the system. This begins by installing Windows 2000 SP2. When installing this update, choose not to backup the original files. It either is or is not going to work correctly. If it does not work correctly, it is much more worth the time to fix the problem instead of rolling back to a previous service pack that will not be supported by Microsoft.

Installation of Internet Explorer 6 and other software

The next step is to bring the browser up to the latest supported version. This is because Microsoft releases patches for the latest versions quicker. Either install using a CD or over the Internet. Again, remember to install only the options that are needed to access the corporate web server. Even though it will not be used, I would suggest upgrading Window Media Player due to the same problem with previous version of Internet Explorer. Vulnerabilities have been found with the Windows Media Player.

Installation of post service pack 2 hot fixes

The quickest way to install the correct hotfixes is to go to http://windowsupdate.microsoft.com of which most users should be familiar with. The patches needed here are the critical ones and the advanced security updates. The compatibility updates are not needed for this installation. Because Internet Explorer is the only software that will be used on this system, software compatibility updates are not needed.

Setting up the kiosk login account and administrator account changes

Create a user that is only a member of "Guests" and check the boxes "User cannot change password" and "Password never expires". All users will use this account

to log into the system. The user cannot change the password for obvious reasons. There is no need to expire the password since everybody will need it to access the system, and it will most likely always be posted near the terminal anyway. Since the administrator account will be used for maintenance and changed on a normal basis as per company requirements, make sure "Password never expires" is not checked.

Troubleshooting notes before proceeding any further

You should now have your default installation of Windows 2000 Professional all setup and ready to secure. Log into the system using the kiosk account created above. Here is a quick troubleshooting tip before we get deep into the security modifications: Before you go any further, make sure ALL areas where the user will require access on the community web server can actually be accessed correctly from the user account on the kiosk. It would be a very big waste of time to try to diagnose what the security template broke, only to find out that it did not work correctly to begin with. It seems to be such a simple step, but when overlooked it can really cause a lot of grief!

Windows 2000 and the High Security Template

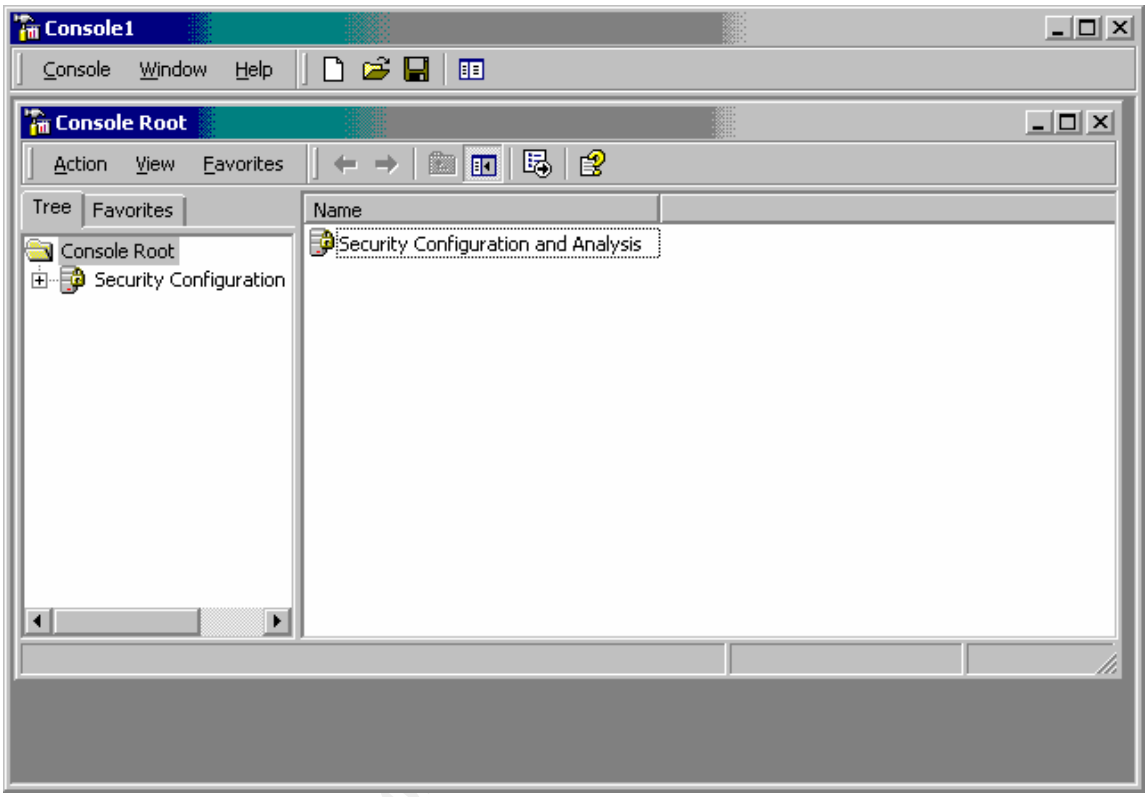
Windows 2000 brought with it a feature to alleviate the headache of trying to remember all the registry entries and other places to go when locking down a system. Window NT 4.0 had the policy editor, and Windows 2000 has the security template that has gone much further in simplifying the application of security changes. Using security templates allows the administrator control over many different aspects of the security of the system from one central point. This also makes it much easier for distribution, instead of having to partially poke around in the registry and hope that an incorrect entry has not permanently disabled the system.

The Microsoft provided high security workstation template (HISECWS.INF) will be applied to strengthen the security of the standard Windows 2000 Professional installation. HISECWS.INF is the highest level of security for a workstation provided in a Microsoft template. This is the template that will be used for the rest of this document. The template will also be changed a little bit for the kiosk implementation.

The "Security Configuration and Analysis" snap-in

Microsoft provides a useful and intuitive GUI tool for working with security templates. This tool is provided as a snap-in for the Microsoft Management Console (MMC). The snap-in is called "Security Configuration and Analysis". With this snap-in the template can be loaded, compared to the current workstation security configuration, changed as needed, and applied to the system. These are the steps for loading this snap-in:

1. Press the "Start" button
2. Click "Run…"
3. Next to "Open:" type MMC.EXE and click "OK". This will open an empty MMC.
4. Hit CTRL+M
5. On the "Add/Remove Snap-in" popup, click "Add…"
6. On the "Add Standalone Snap-in" popup, scroll down and select "Security Configuration and Analysis" then click "Add".
7. Click "Close" to close the "Add Standalone Snap-in", and click "OK" to close the "Add/Remove Snap-in". You will now see the MMC with the analysis tool loaded, similar to the picture below:



This is where all the changes will be made in the following steps. To begin with, click on "Security Configuration and Analysis". The below steps will be presented and should be followed to create a new database:

> ## Security Configuration and Analysis
>
> **To Open an Existing Database**
>
> 1. Right-click the *Security Configuration and Analysis* scope item
> 2. Click **Open Database**
> 3. Select a database, and then click **Open**
>
> **To Create a New Database**
>
> 1. Right-click the *Security Configuration and Analysis* scope item
> 2. Click **Open Database**
> 3. Type a new database name, and then click **Open**
> 4. Select a security template to import, and then click **Open**

When prompted with the "Import Template" popup, select HISECWS and click "Open". This will load the high security template into the database. The system is now ready to be analyzed.

Analyzing the system against the HISECWS security template

Right click "Security Configuration and Analysis" and then "Analyze Computer Now…" to do a comparison of the standard Windows 2000 installation settings to

those set in the HISECWS template. The green checkmarks in the little circles are for settings that are ok. The red "X" marks are on items that will be changed by the security template. The "Database Setting" column consists of the HISECWS template settings, and the "Computer Setting" column lists the standard workstation settings. When a reference in the below sections is made to the security template, this is referencing the "Database Setting" column. For settings that are not mentioned, the high security template values will be used. Go ahead and peruse through all the different security settings to get a feel for all the settings that can be changed. There are quite a lot!

Now we begin the analysis of what is set, why it is set, and possibly why it should be changed. The following section should be read and modified as is appropriate before applying the security changes to the system. The template at the end of this section will be saved, and then applied to the kiosk. Each highlighted title below matches to a setting and/or section in the security analysis tool.

Account Policies – Password Policy

Notice the changes in this area as compared to the default settings. All the changes will be accepted from the security template except for the password length. There has been a long discussion about how long a password should be. Here is one opinion on the subject which was interesting reading:

> "Seven, Eight, or Nine Characters: Which is Most Secure?
>
> A number of theorists have proposed that there is a magic number for Windows passwords. Although in general it is usually true that the longer a password is the harder it is to crack, the Windows LAN Manger (LM) passwords algorithm for encryption gave no more security when passwords were more than seven characters in length. Here's why.
>
> Instead of encrypting a 14-character password, the LM algorithm divided the password into two separate seven-character words and encrypted them separately. Then the halves were combined. This made it easier for the password to be broken because a seven-character password is easier to crack than a 14-character one."[1]

For our situation, we will be using a password of seven characters. The advantage is that a cracking program has to break all or none of the password. If the password was more than seven characters, those characters after seven can be broken separately then used to determine the first part of the password. Since most passwords are still word based in one form or another to be easier to remember, this would allow a hacker to reduce the password analysis time.

Although on first thought it would seem that password complexity is not important, remember the administrator account. Enabling password complexity immediately kills passwords such as "password" and requires a combination of characters such as numbers, uppercase letters, lowercase letters, and even special characters. If this system was hacked through the

[1] Bragg, Roberta, *Windows 2000 Security*, Indianapolis: New Riders Publishing, 2001

administrator account, much more damage could be done than from a regular workstation. Remember that this machine will be used to access personal financial data, and how many people use the same password for more than one type of server access? If the hacker gets one password, that password could be used to log into other internal systems.

Account Policies – Account Lockout Policy

This section will be changed from the security database settings to ease administrative overhead. The password will be made to unlock after 30 minutes instead of permanently locking the account as the settings are on both the system and security template. This will relieve the administrator to do other work instead of having to go and unlock the system when a user forgets the caps-lock is enabled or just keeps mistyping the password. Since the system does unlock, the number of password retries will be reduced from five attempts as suggested by the security template to only three.

Local Policies – Audit Policy

Auditing is much more useful on a workstation with individual logins than a kiosk with a single user login. All events on a kiosk only correspond to one of two accounts. However, it is still very important to log all events to provide a correlation trail to isolate when a kiosk is being abused or used for other purposes. There is still an administrator account that is very vital to the security of the kiosk. It is definitely a good idea to keep an eye out for repeated attempts at trying to log into the system with other account names. The settings suggested by the security template will be used without any changes.

Local Policies – User Rights Assignment

There are no changes in this area by the security template, but for our use one change will be made. All users must be removed from the very first entry: "Access this computer from the network". This will prevent any users from being able to access the machine except by locally logging in and deny access if any shares are ever created on the machine. This is more preventive maintenance than anything else. If an administrator slips and creates a share, no one will be able to connect to it.

Local Policies – Security Options

This area is the most important area for security options. The options of note are as follows:

Additional restrictions for anonymous connections

If this is left at the default setting, a hacker can get a list of users of the system without needing a login and password as long as the server service has been enabled. Although this system will not allow any sharing of resources, it is always a very good idea to disable this ability. The high security template correctly disables anonymous access.

Clear virtual memory pagefile when system shuts down

Enabling this setting clears the pagefile on shutdown. This guarantees that no residual information remains in the pagefile after the system has been shutdown. This also allows a quick cleanup of the pagefile if anything comes into question on the machine and it has to be rebooted. The security template setting of enabled will be used for this setting.

Digital signing/secure digital signing

The key options to be aware of in this area are the digital signing and secure channel communications. These settings do no apply to the system because we will be accessing other possibly non-Windows servers via https most likely through a firewall. This will also apply to secure sessions discussed later in the document. However, it is always good practice to enable signing, so the security template settings will be used.

Disable CTRL+ALT+DEL requirement for logon

The original reason this was created was to prevent keystroke capture programs from showing a bogus login then passing the information on to the real login portion of the operating system. In time and with enough work, the possibility of breaking something gets higher and higher. There are now keyboard capture programs and other such big brother programs that circumvent this requirement. There is still a good reason to keep this disabled: logon text message. If this is enabled, the user never sees the logon message. If the company ever has to prosecute someone, the first item that will be asked of the company is if there was a banner or message on login where the user had to click "OK". The next question will be if it stated that the user consented to monitoring by logging in. Without such a warning, a company does not have the right to monitor users, especially those that are not employed by the company. Keep that in mind whenever creating a logon message – it does happen. The high security template setting of disabled will be used for this setting.

Do not display last user name in logon screen

Enabling this entry ensures that someone does not log on as administrator, then log out leaving the modified administrator account name in the logon screen. This, of course, will be because you renamed the administrator account (keep reading). It makes it much more difficult to hack into a system if the hacker does not know where to start. For this system there will be a dummy “administrator” account just for that reason. Decoys work quite well. The high security template enables this entry, so no changes are needed.

Message title and text box

The security template does not make any changes to these settings because these two boxes are always a little different for each company that sets up Windows 2000. With the system not logging into the domain to get the login messages, a login text box is required with the appropriate company wording. It should at least include something pertaining to the fact that the

user consents to full monitoring, is only using this system as per allowed, and forfeits all rights of data placed on the machine.

Prevent users from installing printer drivers

The security template change will be accepted for this case. It is important to limit user access as much as possible. This is an example of an area that should be denied to the user.

Rename administrator and guest account

As is common security practice, the administrator and guest account will be renamed. There is no need to make it that much easier for someone to know an account worth attacking. The security template does not change this value to prevent renaming these accounts by accident, and if it changed these names in the template, all machines using the HISECWS template would be renamed the same -- what good would that do? For this system, a disabled administrator guest account will be created after renaming the actual account. As a reminder, remember to remove the "Built-in account for administering the computer/domain" and "Built-in account for guest access to the computer/domain" lines after renaming the accounts. It takes a lot of the guesswork out if the renamed account still has the original description with it. When creating the administrator ghost account, use the "Built-in account for administering the computer" line ("…computer/domain" is too long to fit in the description field when creating a new account). Do NOT rename the administrator account to "admin". This is one of the most common used account names for the administrator account.

Unsigned driver installation behavior

Although this can be used as a hack when enabled, it should be left at the computer setting of "Warn but allow installation". This is an instance where reducing the administrative overhead of multiple images weighs out over a hacker placing a modified driver file on the system. For sites with different hardware and printers, a lot of the manufacturer provided software and drivers could not be installed.

Event Log – Settings for Event Logs

The event log is the main utility used to view all audit trails and system messages. In a high security environment, a large amount of system processes, files, and other portions of the operating system are logged. When creating a kiosk, these logs are not as significant but still are important. The kiosk only has two accounts that are not locked down to a specific user at the console. The event logs will display someone trying to break into the kiosk or succeeding, but there will be no further useful information to determine whom the perpetrator is.

Maximum application and system log size

Due to the small footprint needed on a system for a kiosk, the logs can be increased without any problem to maintain a better history of problems. The computer setting will be increased from 512k to 4096k. The security template does not make any changes to the computer settings.

Restrict guest access to application, security and system log

No changes need to be made to the security template settings. Notice the template restricts access to all event logs. Even on a normal workstation, these settings should be enabled. Why would a guest user need access to the logs in the first place? On a kiosk, this is even more important. The user does not need to know what is and is not being audited. Viewing the logs would also allow trend analysis of times when users use the system and when the administrator logs in for maintenance.

Retention method for application, security and system log

The security template value will be used for all logs, not just the security log. Since this is kiosk, it should be as self-sustaining as possible. That means that the administrator should not have to be notified when an error message pops up every time a user logs on. To guarantee this, the retention method will be set to overwrite as needed for all portions of the event log. This is the reason the log sizes were increased earlier. Although data will be overwritten, the idea is that enough data will be preserved for the auditing trail. Setting the logs to overwrite as needed will remove the "Log file is full" error message on boot.

Restricted Groups

This are of the security template should not be modified. If changes were made here, the administrators setting up the kiosk machines would probably need to be educated on the differences from the standard workstation setup they are used to. There is no need to create this extra step of confusion for the administrators who have little spare time as it is.

System Services

Here is the area where things get interesting. As per the high security template, none of the service startup parameters are modified. For a kiosk, only the essential operating system services should be running. The problem here is creating a balance between needed services and securing the system. The best way to secure system services is to actually disable the service so it cannot be started locally or remotely. With that information in mind, below begins the changes to the services including the reason of why or why not the change is needed.

Application Manager

This service provides the ability to install software. The idea of the kiosk is not to allow any other software to be installed. Even though this system will not be part of an active directory, the service will still be disabled.

ClipBook

This is another remote ability service. No remote connections are allowed, so this service will be disabled.

DHCP Client

In this company, DHCP is not allowed. The reason for this is the problem of isolating a problem user on a weekly basis. There are ways to lock down DHCP as needed (for example, by MAC address), but for the other monitoring and reporting software used, a static addressing scheme works much easier. The service is set to disabled so that the administrator must give the system a static IP address.

Fax Service

It should be very easy to figure out why this service should be disabled. The kiosk will definitely not need to be able to send and receive faxes. Disable the service.

Indexing Service

This service adds no value to the kiosk. It provides the ability to perform quick custom searches of files on the hard drive. Since the user will not need this access, the service will be disabled.

Internet Connection Sharing

This is another obvious service to disable. If enabled on a system with two network interface cards (NICs), the system will act as a router so that any computer on the second NIC segment can point to the dual-NIC system and get to networks that the dual-NIC system by itself can reach. This service will be disabled.

NetMeeting Remote Desktop Sharing

This is another dangerous service to have enabled. If the user enables NetMeeting for desktop sharing, the system can be logged into the same way as a system running Terminal Server. The service will be disabled.

Remote Access Auto Connection Manager

This system will only be accessing sites by SSL. Remote access will not be required. This service will be disabled.

Remote Access Connection (RAS) Manager

This service falls under the same rules as the above. With only a need for web based access, RAS is not needed.

Remote Procedure Call (RPC)

This service should NOT be disabled at all costs. This is the heart of Microsoft communications both across the network and on the local machine. If this service is disabled, many other services will also fail. One of the more important services that will fail is the “Protected Storage” service. This service handles much of the transfers on the hard drive. If this service does not start, the system runs in slow motion and will almost

grind to a complete halt. There are a total of fifteen different services that have a dependency on this service.

Remote Registry Service

Anything that allows remote ability does not need to be running on a kiosk. This service allows working with the registry from another workstation. This service will be disabled.

Task Scheduler

This service allows the ability to run tasks at set times. The kiosk in this example will not have any maintenance scripts running, except at boot-up and logon. There is no need for this service, so it will be disabled.

TCP/IP NetBIOS Helper Service

This service allows NetBIOS over TCP/IP, which should not be enabled on the kiosk. This service also provides NetBIOS name resolution (WINS), so if this was connecting to a corporate web server, the server would require a DNS name. Because we are connecting to a community server not even on the local network, there is no need for this service. This service will be disabled.

Remember to disable this ability on the NIC to prevent an error message in the event log. To do this, open up the properties on the network card and select "Internet Protocol (TCP/IP)". Click the "Properties" button, then the "Advanced…" button, and finally click the "WINS" tab. Check the radio button next to "Disable NetBIOS over TCP/IP". This will prevent the machine from using this service when booted.

Telephony

This service is the backbone for all Telephone API (TAPI) products. The most common programs that use this service are NetMeeting and PhoneDialer. With these programs, the user can contact other systems on the Intranet and Internet, and also receive calls. The kiosk in this example will never be setup to receive communications of any sort. This service will be disabled.

Telnet

Windows 2000 now has the ability to allow telnet access to the machine, which was probably brought on by the request of the many Unix users out in the world. As has been proven by multiple vulnerabilities, Microsoft still has a lot of work to make it a safe way to access the system. This is not really a surprise; Microsoft just got into using telnet, and Unix and other operating systems have had telnet access for years of which vulnerabilities still occasionally appear.

The idea behind the use of telnet access is the position by Microsoft that as many tasks as possible should be able to be accomplished from the command line or via script. Microsoft still has a ways to go, but Windows

2000 has had some major improvements in this area. For the kiosk, though, all telnet access will definitely be denied. This service will be disabled.

Registry

This area of the template turns on auditing and changes permission in different areas of the registry. For the purpose of the kiosk, the security template settings will be used. The main change that is made to the registry keys is to remove some of the administrative ability of the power users group on the workstation and make them closer to a regular user account.

File System

The purpose of this area of the analysis tool is to allow the user the ability to change auditing, individual permissions, inheritance, and propagation of files and directories on the hard drive. Once the high security template is applied, only two areas of the file system will be changed.

C:\

The first change to make is to deny write access except to the service account and the administrators group on the root of the drive. The high security template does not perform this modification. Remove the Everyone group, and add the administrators, SYSTEM, and Users groups. The default permission when adding these accounts is to allow only "Read and Execute", "List Folder Contents", and "Read". These permissions will work without any modifications except for the administrators group and SYSTEM group. These two groups need the "Full Control" box checked. Any new folders created off the root will also have these permissions.

Document and Settings

The security template does not make any changes to this directory. Remove the Everyone group, and add the administrators, authenticated users, CREATED OWNER, SYSTEM, and Users groups. The default permission when adding these accounts is to allow only "Read and Execute", "List Folder Contents", and "Read". These permissions will work without any modifications except for the administrators, CREATED OWNER, and SYSTEM group. These three groups need the "Full Control" box checked.

Program Files

The security template actually smoothes out the inconsistencies of permissions in this directory, and will be used without any changes. Instead of a mixture of inherited and non-inherited permissions, the security template changes the files and directories to inherit the permissions of the "Program Files" root directory. This makes it much easier to determine the rights a user account has to the directory structure and files. Upon close examination, the files actually do have the same permissions as the "Program Files" root. The only difference is that the

permissions were not inherited from the previous directory. The last change to take note of is that the power users group is changed to have the same permission access ability as a user. The power user no longer has any special rights higher than the user to this directory structure.

WINNT

The only change to this directory by the security template is to remove some of the rights of the power users group to make them equal to the regular users group. For the kiosk, more changes will be made. The only change to the security template will be the removal of the "Everyone" group.

WINNT directories: Addins, Connection Wizard, Java, MSAgent, Repair, Speech, System32, Temp and Twain_32

The power user is made equivalent to the user on the permissions on these directories. The only part in question to these directories is that the permissions on WINNT are the same on these directories, yet the rights are not inherited. This was probably done to match the non-inherited rights flow of the default operating system install. No changes to the security template will be made on these sections.

WINNT directory: AppPatch

This directory has the same removal of power user rights, but also now inherits the permissions from the WINNT directory. Something of note here is that the EVERYONE group has been removed once the security template has been applied. No changes to the security template will be made on this section.

WINNT directory: Driver Cache

This directory has an odd change to it by the security template. It gives the "CREATED OWNER" access to the current folder, instead of only the subfolder and files limited by the standard Windows 2000 install. For this install, the security template setting will be changed back to the standard Windows 2000 settings for "CREATED OWNER" and check the box "Do not allow permissions on this file or folder to be replaced".

WINNT directory: Installer

Unlike the previous folders, the Installer folder is changed to inherit the permissions from the WINNT directory by the security template. This is actually a beneficial change because the default permission is to allow everyone to read, list and execute any files in this directory. With the inherited permissions, the "Everyone" group is denied access to the directory.

Backing up and applying the modified security template

Now that the template has been completed, it needs to be backed up and applied to the system. Export the template using the "Export template…" command, and

save it on the hard drive. Before continuing any further, put a copy of the file on a floppy disk and remove it from the system so you have a backup in case everything goes crazy.

The template can now be applied to the system. Left-click "Security Configuration and Analysis" and choose "Configure Computer Now…". It will take a moment while all the changes are applied. Once it has been completed, reboot the system and log in using your new administrator account.

User account modifications

Now that the system has been secured, a few more actions need to be performed on the kiosk.

Creating a dummy administrator account

This is one of the more common practices in the security world. The administrator account has already been renamed, but if a hacker can figure this out, the hacker will go after other accounts on the machine. To make this a little more confusing, an account will be made with the name "administrator" with the description "Built-in account for administering the computer". Notice that the built in account has "…administering the computer/domain". When creating an account, there is not enough space to put back in this entire description. Just think of it as another Microsoft "feature". This new administrator account will have a very tough password, only belong to the guest users group and be disabled. It should keep the hackers busy for a while.

Changing the renamed administrator and guest accounts descriptions

In the previous template, the default administrator and guest accounts were renamed. This is helpful in securing the system, but the default description still followed the accounts. The last step to modify on these accounts is to remove the descriptions.

Analyzing the High Security Template

The high security template with modifications has now been applied to the system. Now that the system has been secured using the template, the next step is to analyze what we have done with the template and what we want to accomplish with it.

Applying the high security template to kiosks

This image will be distributed to the field with the original high security template already applied. This image will wipe the current hard drive in the system and replace it with the kiosk image. Distribution in this manner will have the lowest administrative overhead; the install will simply consist of a bootable CD and a hard drive image file.

Updates to the high security template

A unique problem with these systems is how to update the template when changes are needed. Unfortunately, it will have to be accomplished by the local technician. Because we have removed as much network access as possible, there is no way to remotely update the system. This was the disadvantage of removing all remote access for security reasons; security took a much higher priority than administration. Any program used to remotely update the system could also be used to compromise the security of the system. Updated templates will have to be supplied to the technician, who will log into the machine as the administrator and apply the changes. Changes to the template should be minimal, so there should not be much work required on the technician's part to apply the updated template. What the technician will have to constantly update is the operating system as security patches and other patches are released. These patches (including the template updates) will be supplied via CD-ROM to the local technician to update the system as needed since the kiosk will only have access to the community web server.

Testing system changes made by the high security template

Now that we have decided how to distribute the template, it is time to make sure the template limited access as it was supposed to. We will perform a few tests to make sure access is denied properly.

Creating a share to a Microsoft resource

The first test is to guarantee that the user cannot connect to another Microsoft operating system using a remote procedure call (RPC). If this was accomplished, the user could access another server to create problems, and there would be no distinct username to match the attack to (except for the kiosk user or administrator account). The kiosk will also only be used for SSL access to another server not on the local network that will never require access via RPC calls. There are multiple ways to create shares on Windows 2000. For this test, the command prompt and "My Network Places" on the desktop were used.

The first test was to create a share from the command prompt. This was performed by attaching using the command "net use <drive letter> <share>". The following error message was returned when executing this command:

C:\>net use v: \\172.16.8.19\c$

The Workstation service has not been started.

More help is available by typing NET HELPMSG 2138.

This is the expected system response to the above command. The workstation service was removed by uninstalling the client for Microsoft networks. Typing NET HELPMSG 2138 at the prompt gives the following explanation:

C:\>net helpmsg 2138

The Workstation service has not been started.

EXPLANATION

You have tried to use the network before starting the

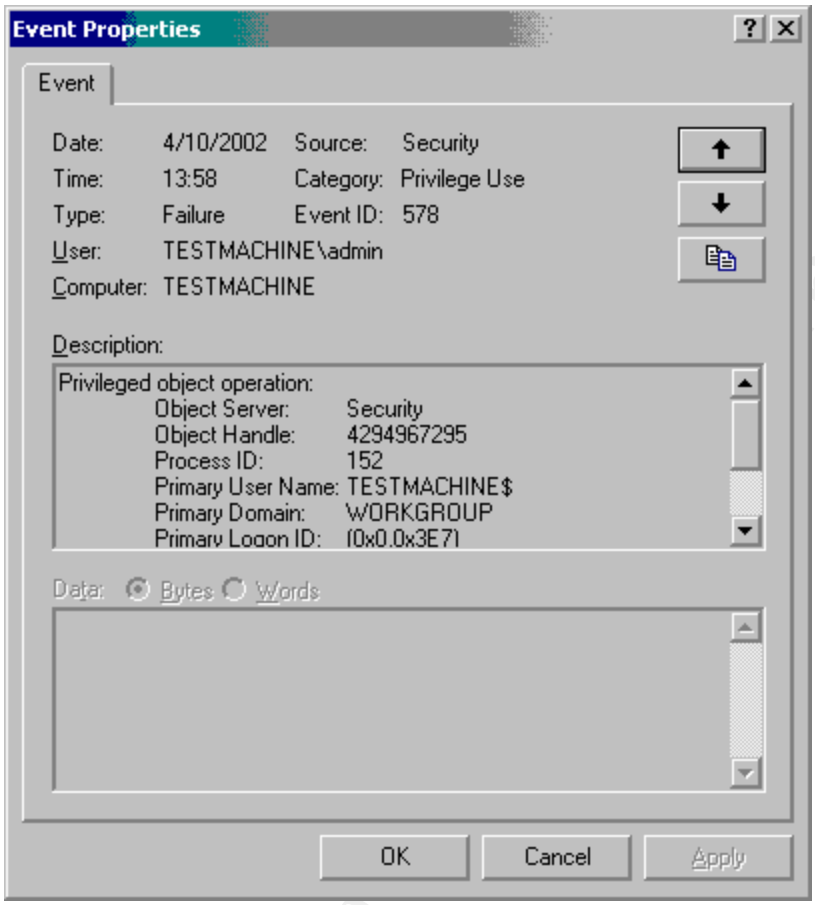
Workstation service.

ACTION

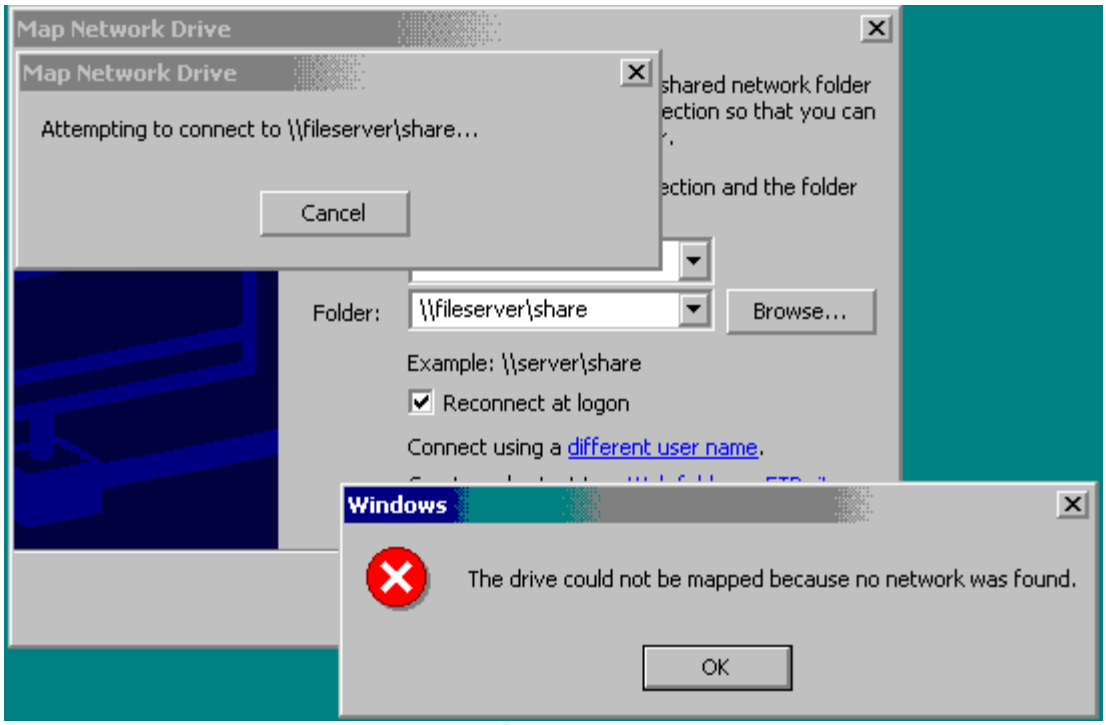
Start the Workstation service by typing:

NET START WORKSTATION

The associated logged entry in the event viewer is show below. Notice the "Type: Failure" in the image.



Here is the same response when trying to create a share by right clicking "My Network Places" and choosing "Map Network Drive".

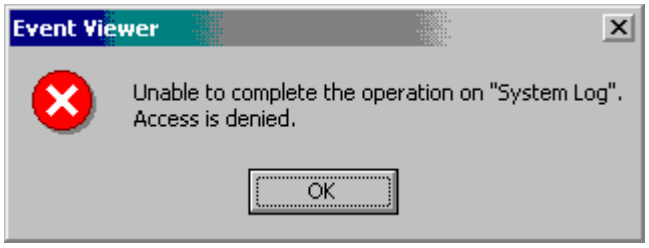


The network could not be found because the workstation service could not be used to attempt a Microsoft client connection. Both these tests were performed from the administrative account. The same message would be displayed if attempted from the kiosk user account.

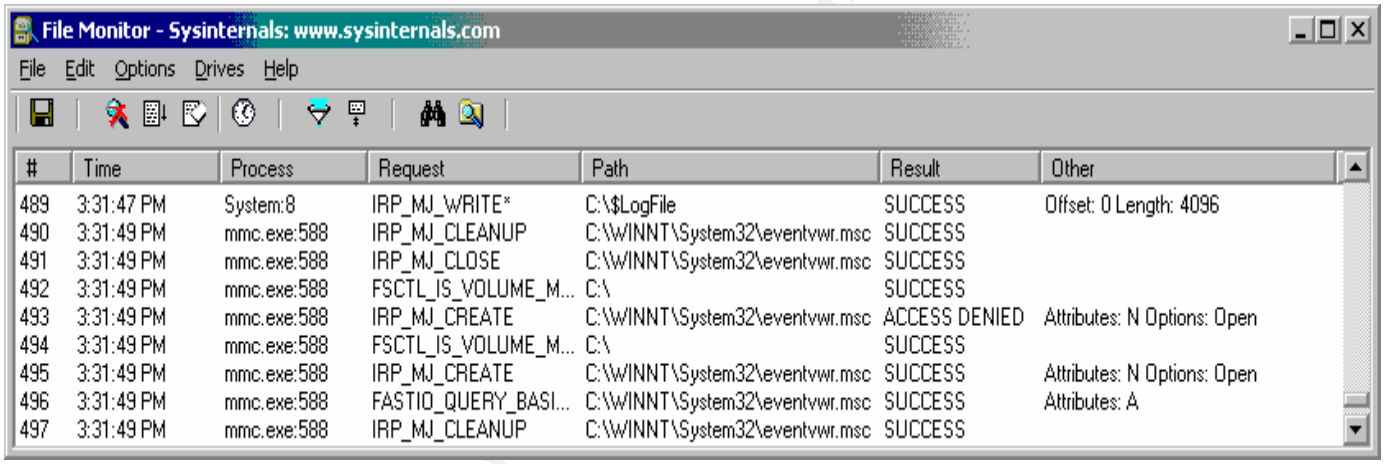
Here is some more detailed information about the workstation and related remote procedure call (RPC) service. The exact problem is that the transport – an RPC connection using the workstation service – is not available to create the necessary connection. This is because the workstation service has been totally removed from the NIC bindings. Remember that this does not kill all server accessibility, only those requiring a Microsoft workstation login such as a share. The RPC service is quite powerful and does not need the workstation service for some remote connections. An example of this is connecting to an Exchange server with an RPC connection; the workstation is not a member of the domain and only needs to have a valid username and password – the workstation service does not have to be enabled for the connection through Outlook to succeed. An attempt was made to disable this ability by disabling the RPC service, but Windows 2000 is much more dependent on the service that Windows NT. The system almost died instantly one the RPC service was disabled; as compared to Windows NT where the service can be removed without any problem. There are other types of connections that can be made using only the RPC service (this was the idea behind the service), so keep this in mind when trying to limit system access.

Guest user viewing of event logs

The next test is the denial of a guest to view the event logs. There is absolutely no reason for a guest user to be able to view the event logs. Using the security template, this ability has been disabled. Below is a screen shot of the error message when the kiosk account is used to access the system log in the event viewer. The same message is presented when the application and security logs are viewed.



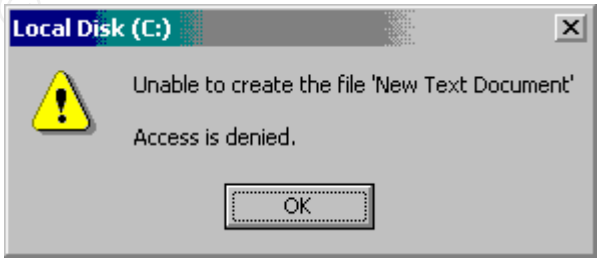
Using a file monitor tool, we can see that the user is actually denied access to the eventviewer file on the hard drive. The same error messages showed up whether the event viewer was pulled up through the administrative tools (uses the MMC) or running the shortcut from the command line (eventvwr.msc).



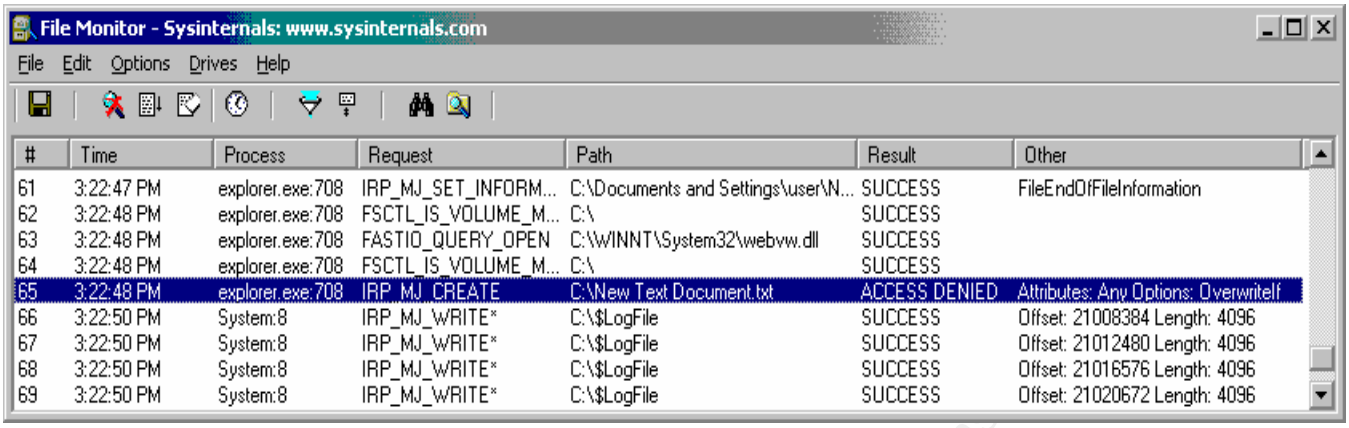
#	Time	Process	Request	Path	Result	Other
489	3:31:47 PM	System:8	IRP_MJ_WRITE*	C:\$LogFile	SUCCESS	Offset: 0 Length: 4096
490	3:31:49 PM	mmc.exe:588	IRP_MJ_CLEANUP	C:\WINNT\System32\eventvwr.msc	SUCCESS	
491	3:31:49 PM	mmc.exe:588	IRP_MJ_CLOSE	C:\WINNT\System32\eventvwr.msc	SUCCESS	
492	3:31:49 PM	mmc.exe:588	FSCTL_IS_VOLUME_M...	C:\	SUCCESS	
493	3:31:49 PM	mmc.exe:588	IRP_MJ_CREATE	C:\WINNT\System32\eventvwr.msc	ACCESS DENIED	Attributes: N Options: Open
494	3:31:49 PM	mmc.exe:588	FSCTL_IS_VOLUME_M...	C:\	SUCCESS	
495	3:31:49 PM	mmc.exe:588	IRP_MJ_CREATE	C:\WINNT\System32\eventvwr.msc	SUCCESS	Attributes: N Options: Open
496	3:31:49 PM	mmc.exe:588	FASTIO_QUERY_BASI...	C:\WINNT\System32\eventvwr.msc	SUCCESS	Attributes: A
497	3:31:49 PM	mmc.exe:588	IRP_MJ_CLEANUP	C:\WINNT\System32\eventvwr.msc	SUCCESS	

Writing to a restricted directory by the kiosk user

We will attempt to write to a directory that the kiosk account only has read access to. For this example, the root directory "C:\" will be used. Copying a file to the root of the hard drive from the kiosk account gives the following error message:



Using a utility to watch the file access on the hard drive, it can be seen that the file creation attempt is denied.

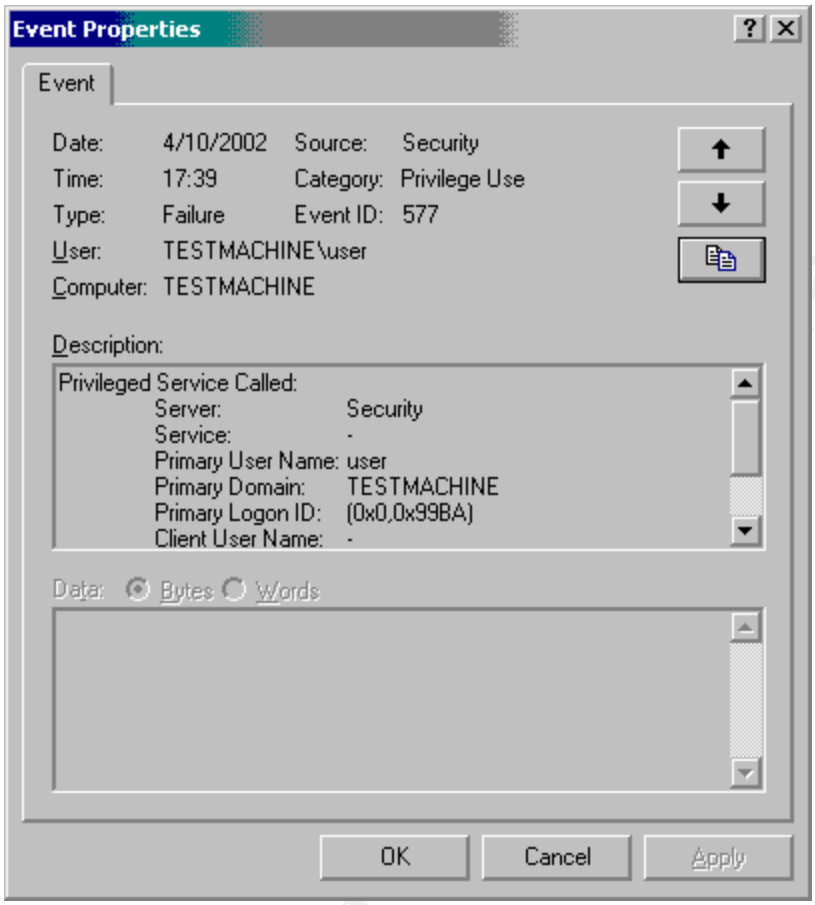


The permission change was applied successfully to the root of the hard drive.

Adding a printer with the kiosk user account

The kiosk user setup as a guest account will not be allowed to add a printer. This configuration will only belong to the administrative account on the machine. Permissions are not checked until the printer is created in the registry, so the user may think a printer has been successfully created until the very last step. The following is the message shown to the user:

This is the permission error logged in the security portion of the event viewer:



As can be seen by the above failure message, the guest was correctly denied the ability to add a printer.

Testing the required applications for correct functionality

Now that we have tested a few of the policy changes for correctly being applied, we now need to make sure the essential tools needed on the kiosk have not been broken. Below are some tests of the operating system to guarantee the correct operation of areas vital to the kiosk.

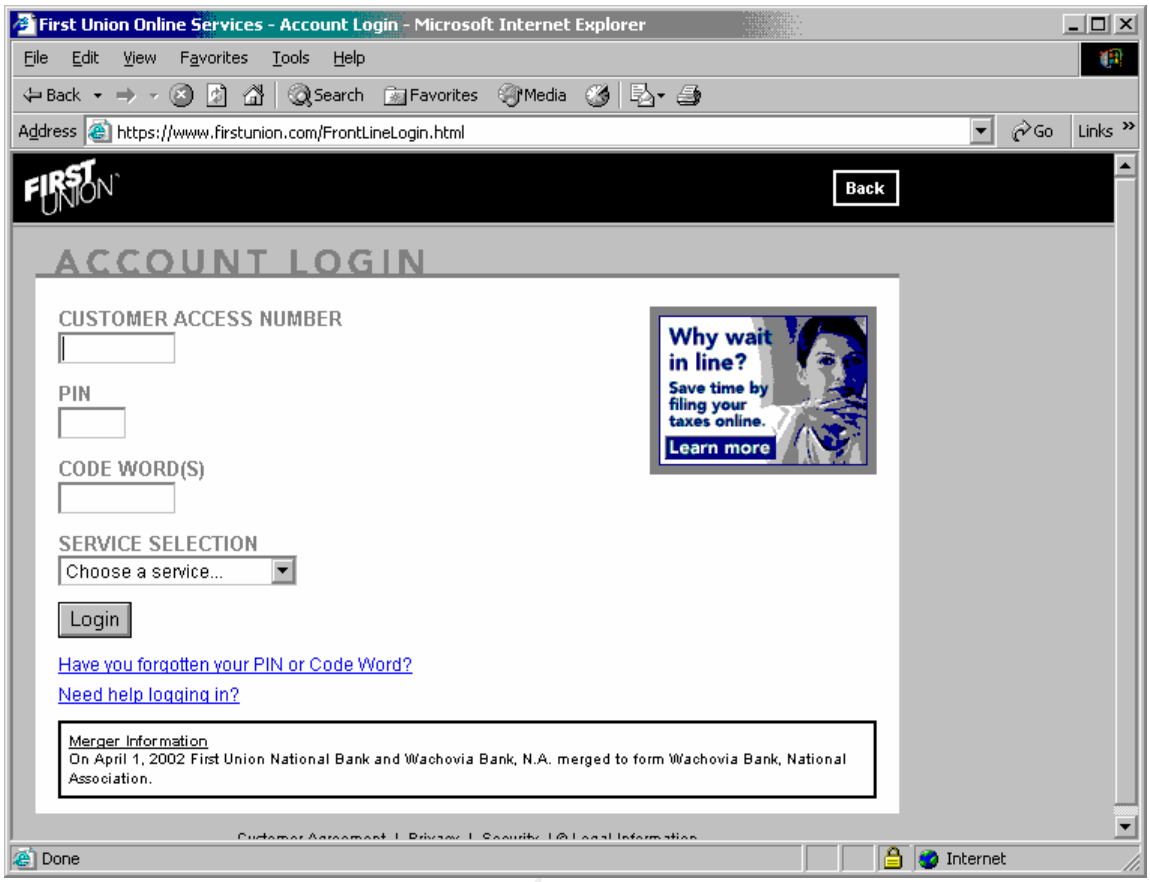
Adding a printer

This system has been designed to allow the user to access the community web server and print out personal information. To enable the user to do this, there is a requirement to have a printer locally attached to the system. Without this ability, the kiosk is useless therefore this must be tested. As tested above, the kiosk user was not able to add a printer. Here, we are making sure the administrator can add a printer. Below is a screen shot showing the successful addition of a printer.

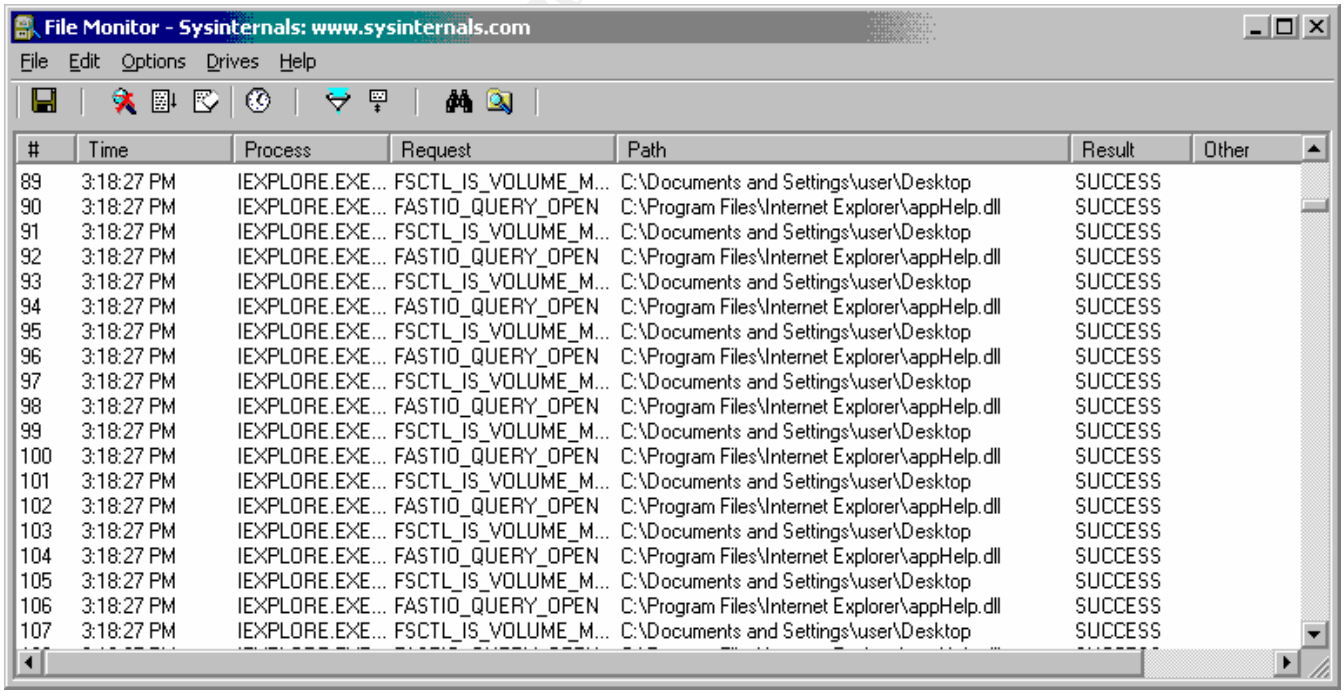
Now that the printer has been installed, test it to make sure everything prints out correctly. In this test kiosk, the system printed without any problems from the administrator account.

Correctly functioning Internet Explorer

The next test is to make sure the application the kiosk was made for still functions correctly. For our example, the only software package we are concerned about is Internet Explorer. Log into the machine using the kiosk user account and access the community web server. Below is a screen shot of an example community financial access point:



And below is a screen shot of the permission accepted for running IEXPLORE.EXE (the Internet Explorer executable):



#	Time	Process	Request	Path	Result	Other
89	3:18:27 PM	IEXPLORE.EXE...	FSCTL_IS_VOLUME_M...	C:\Documents and Settings\user\Desktop	SUCCESS	
90	3:18:27 PM	IEXPLORE.EXE...	FASTIO_QUERY_OPEN	C:\Program Files\Internet Explorer\appHelp.dll	SUCCESS	
91	3:18:27 PM	IEXPLORE.EXE...	FSCTL_IS_VOLUME_M...	C:\Documents and Settings\user\Desktop	SUCCESS	
92	3:18:27 PM	IEXPLORE.EXE...	FASTIO_QUERY_OPEN	C:\Program Files\Internet Explorer\appHelp.dll	SUCCESS	
93	3:18:27 PM	IEXPLORE.EXE...	FSCTL_IS_VOLUME_M...	C:\Documents and Settings\user\Desktop	SUCCESS	
94	3:18:27 PM	IEXPLORE.EXE...	FASTIO_QUERY_OPEN	C:\Program Files\Internet Explorer\appHelp.dll	SUCCESS	
95	3:18:27 PM	IEXPLORE.EXE...	FSCTL_IS_VOLUME_M...	C:\Documents and Settings\user\Desktop	SUCCESS	
96	3:18:27 PM	IEXPLORE.EXE...	FASTIO_QUERY_OPEN	C:\Program Files\Internet Explorer\appHelp.dll	SUCCESS	
97	3:18:27 PM	IEXPLORE.EXE...	FSCTL_IS_VOLUME_M...	C:\Documents and Settings\user\Desktop	SUCCESS	
98	3:18:27 PM	IEXPLORE.EXE...	FASTIO_QUERY_OPEN	C:\Program Files\Internet Explorer\appHelp.dll	SUCCESS	
99	3:18:27 PM	IEXPLORE.EXE...	FSCTL_IS_VOLUME_M...	C:\Documents and Settings\user\Desktop	SUCCESS	
100	3:18:27 PM	IEXPLORE.EXE...	FASTIO_QUERY_OPEN	C:\Program Files\Internet Explorer\appHelp.dll	SUCCESS	
101	3:18:27 PM	IEXPLORE.EXE...	FSCTL_IS_VOLUME_M...	C:\Documents and Settings\user\Desktop	SUCCESS	
102	3:18:27 PM	IEXPLORE.EXE...	FASTIO_QUERY_OPEN	C:\Program Files\Internet Explorer\appHelp.dll	SUCCESS	
103	3:18:27 PM	IEXPLORE.EXE...	FSCTL_IS_VOLUME_M...	C:\Documents and Settings\user\Desktop	SUCCESS	
104	3:18:27 PM	IEXPLORE.EXE...	FASTIO_QUERY_OPEN	C:\Program Files\Internet Explorer\appHelp.dll	SUCCESS	
105	3:18:27 PM	IEXPLORE.EXE...	FSCTL_IS_VOLUME_M...	C:\Documents and Settings\user\Desktop	SUCCESS	
106	3:18:27 PM	IEXPLORE.EXE...	FASTIO_QUERY_OPEN	C:\Program Files\Internet Explorer\appHelp.dll	SUCCESS	
107	3:18:27 PM	IEXPLORE.EXE...	FSCTL_IS_VOLUME_M...	C:\Documents and Settings\user\Desktop	SUCCESS	

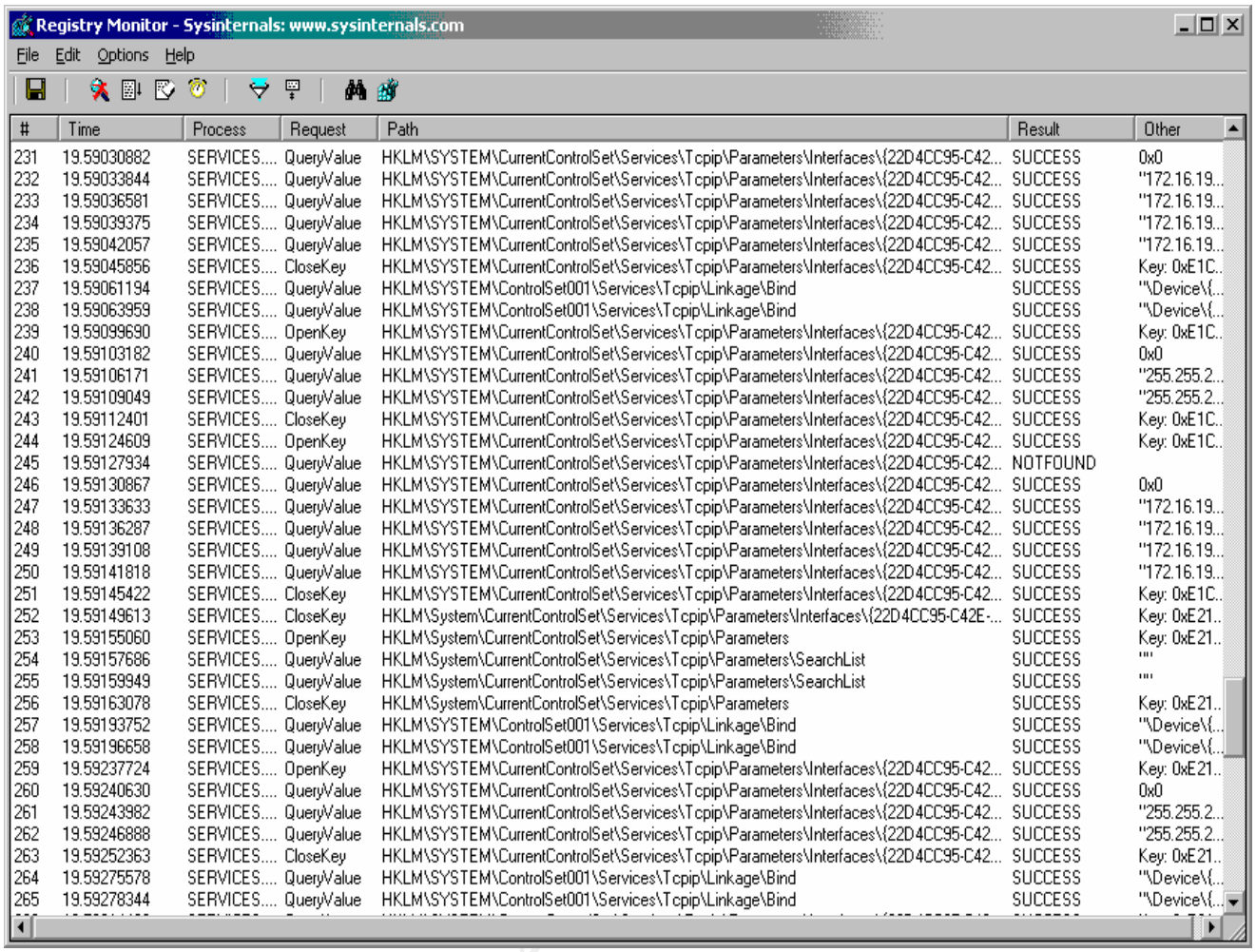
Notice the log viewer does not have any permission errors, and Internet Explorer is running correctly in the task manager. The next step is to log into the community server with an actual username and password and test all areas of the web page to make sure they still work. Once this has been completed to your satisfaction, it is time to test another part of the kiosk.

Printing from the kiosk account

Now that Internet Explorer has function correctly, log into the machine using the kiosk user account a print something on the community web server. On the test machine, this worked without any problems. Remember to always test this; some printers with manufacturer supplied drivers instead of Windows 2000 drivers do not allow enough permission for a user or guest account to print to the printer.

Changing the network properties of the kiosk

In an environment where the security template will be applied to existing machines, making network changes would not be so important. For our example, a single image will be distributed to all sites. Once the site applies the image to whatever hardware is available, the IP address, gateway, and DNS entries must be changed. The primary reason these changes should be tested with the application of the security template is because many services that normally start up have been disabled. Below is a snapshot of the registry changes successfully applied after making a change to the IP address of the network interface. As can be seen, this worked successfully.



#	Time	Process	Request	Path	Result	Other
231	19.59030882	SERVICES....	QueryValue	HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{22D4CC95-C42...	SUCCESS	0x0
232	19.59033844	SERVICES....	QueryValue	HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{22D4CC95-C42...	SUCCESS	"172.16.19...
233	19.59036581	SERVICES....	QueryValue	HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{22D4CC95-C42...	SUCCESS	"172.16.19...
234	19.59039375	SERVICES....	QueryValue	HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{22D4CC95-C42...	SUCCESS	"172.16.19...
235	19.59042057	SERVICES....	QueryValue	HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{22D4CC95-C42...	SUCCESS	"172.16.19...
236	19.59045856	SERVICES....	CloseKey	HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{22D4CC95-C42...	SUCCESS	Key: 0xE1C...
237	19.59061194	SERVICES....	QueryValue	HKLM\SYSTEM\ControlSet001\Services\Tcpip\Linkage\Bind	SUCCESS	"\Device\{...
238	19.59063959	SERVICES....	QueryValue	HKLM\SYSTEM\ControlSet001\Services\Tcpip\Linkage\Bind	SUCCESS	"\Device\{...
239	19.59099690	SERVICES....	OpenKey	HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{22D4CC95-C42...	SUCCESS	Key: 0xE1C...
240	19.59103182	SERVICES....	QueryValue	HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{22D4CC95-C42...	SUCCESS	0x0
241	19.59106171	SERVICES....	QueryValue	HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{22D4CC95-C42...	SUCCESS	"255.255.2...
242	19.59109049	SERVICES....	QueryValue	HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{22D4CC95-C42...	SUCCESS	"255.255.2...
243	19.59112401	SERVICES....	CloseKey	HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{22D4CC95-C42...	SUCCESS	Key: 0xE1C...
244	19.59124609	SERVICES....	OpenKey	HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{22D4CC95-C42...	SUCCESS	Key: 0xE1C...
245	19.59127934	SERVICES....	QueryValue	HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{22D4CC95-C42...	NOTFOUND	
246	19.59130867	SERVICES....	QueryValue	HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{22D4CC95-C42...	SUCCESS	0x0
247	19.59133633	SERVICES....	QueryValue	HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{22D4CC95-C42...	SUCCESS	"172.16.19...
248	19.59136287	SERVICES....	QueryValue	HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{22D4CC95-C42...	SUCCESS	"172.16.19...
249	19.59139108	SERVICES....	QueryValue	HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{22D4CC95-C42...	SUCCESS	"172.16.19...
250	19.59141818	SERVICES....	QueryValue	HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{22D4CC95-C42...	SUCCESS	"172.16.19...
251	19.59145422	SERVICES....	CloseKey	HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{22D4CC95-C42...	SUCCESS	Key: 0xE1C...
252	19.59149613	SERVICES....	CloseKey	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{22D4CC95-C42E-...	SUCCESS	Key: 0xE21...
253	19.59155060	SERVICES....	OpenKey	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters	SUCCESS	Key: 0xE21...
254	19.59157686	SERVICES....	QueryValue	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\SearchList	SUCCESS	""
255	19.59159949	SERVICES....	QueryValue	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\SearchList	SUCCESS	""
256	19.59163078	SERVICES....	CloseKey	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters	SUCCESS	Key: 0xE21...
257	19.59193752	SERVICES....	QueryValue	HKLM\SYSTEM\ControlSet001\Services\Tcpip\Linkage\Bind	SUCCESS	"\Device\{...
258	19.59196658	SERVICES....	QueryValue	HKLM\SYSTEM\ControlSet001\Services\Tcpip\Linkage\Bind	SUCCESS	"\Device\{...
259	19.59237724	SERVICES....	OpenKey	HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{22D4CC95-C42...	SUCCESS	Key: 0xE21...
260	19.59240630	SERVICES....	QueryValue	HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{22D4CC95-C42...	SUCCESS	0x0
261	19.59243982	SERVICES....	QueryValue	HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{22D4CC95-C42...	SUCCESS	"255.255.2...
262	19.59246888	SERVICES....	QueryValue	HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{22D4CC95-C42...	SUCCESS	"255.255.2...
263	19.59252363	SERVICES....	CloseKey	HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{22D4CC95-C42...	SUCCESS	Key: 0xE21...
264	19.59275578	SERVICES....	QueryValue	HKLM\SYSTEM\ControlSet001\Services\Tcpip\Linkage\Bind	SUCCESS	"\Device\{...
265	19.59278344	SERVICES....	QueryValue	HKLM\SYSTEM\ControlSet001\Services\Tcpip\Linkage\Bind	SUCCESS	"\Device\{...

Correct kiosk access summary

The most important tools needed for the kiosk were tested above. Internet Explorer was tested for accessing the community server, a printer was added and used through the kiosk account, and the network settings were changed to the local network. If there are any other essential tools to your implementation, always remember to test them even if other settings should not have had any effect on the tool. You may find a case where Microsoft made a mistake or the manufacturer never intended the hardware to be used except under the administrator account.

Microsoft High Security Template Evaluation

The high security workstation template is supplied as a starting point for a high security of lockdown on a workstation. This template was used as the starting point for increasing the security level of our kiosk system. The template itself is quite useful and did not need a lot of changes.

Changes from the default security template

Changes made from the HISECWS.INF file are listed below. All other settings made by the template were not changed.

Account Policies – Password Policy

This was changed from the template setting of 8 to 7. This was done because Windows stores passwords as characters 1-7 and then 8-14. Using 7 passwords, the password must be an all or nothing. If 8 characters are used, the eighth character can be broken on its own to figure out what the rest of the password is.

Account Policies – Account Lockout Policy

This security template setting was changed to allow the password to unlock after 30 minutes. This was done to ease a little bit of the administrative overhead.

Local Policies - User rights assignment

All entries were removed from the “Access this computer from the network”. The security template did not modify the standard install setting. This disables users from accessing a system over the network using RPC connections.

Message title and text box

The security template did not change this setting on purpose. These two entries have to be entered by the administrator due to every message at login being a little different.

Renaming administrator and guest account

The security template did not change this setting on purpose. If it did, everybody would know the new account names (all Windows 2000 machines have the same high security template).

Unsigned driver installation behavior

The security template set this value at “Do not allow”. For our purposes, it must be set at "Warn but allow installation" so the administrator can install needed hardware and software drivers that may not be signed by the manufacturer.

Maximum application and system log size

The security template changed the security log size, but not the other logs. We increased the other logs to 4096k to have a better history.

Retention method for application, security and system log

The security template only changed the security log to rollover as needed. To prevent users having messages popup that the event log is full, this value has been applied to the application and system log.

System services

The security template made no changes to the system services because some of these changes could cause drastic problems, depending on the use of the workstation. For our use, many of the services that were not essential to the operating system were disabled.

Directory permission changes

This is the only area where changes that should have been made were not by the security template. The template would have been perfect for making a workstation highly secure if the permission of "Everyone" had been removed. The "Authenticated Users" group was added and has been around since Windows NT 4.0 service pack 3. One of the primary reasons for adding this group was to replace using the "Everyone" group for open shares. I am surprised that Microsoft did not use "Authenticated Users" anywhere when applying permission to directories and files on the hard drive. This was most likely an oversight by Microsoft or a decision made for software compatibility reasons.

Overall comments on the HISECWS.INF template provided by Microsoft

The HISECWS.INF template supplied by Microsoft does a good job at securing a workstation. The only issue with the template is the removal of at least the "Everyone" group from the hard drive as mentioned above. Microsoft did a good job on putting this template together and adding all the settings available through the "Security Configuration and Analysis" tool. This template could be applied to a general users workstation without any modifications, and the user would be able to continue using the system with a minimal problems. What made the template work even better was the use of the Microsoft supplied browser Internet Explorer. Remember that the more non-standard software packages that are installed on a system, the more potential problems there will be when locking down the system. The majority of problems with non-standard applications is permissions. The most problematic applications simply want the user to have administrative rights so hard drive permissions do not need to be considered (as is the case with the Windows 9x based versions).

Other items of importance

Now that the security template has been successfully applied and tested, the security of the system has been much improved. Before continuing, here are some reminders as you work on the kiosk that will save you in the long run.

Kiosk user account as a member of Guests reminder

This has already been mentioned multiple times through the document, but I will mention it again. The kiosk user account is setup as a guest account; therefore the profile is created from scratch at every login. That means the user profile has to be modified via scripts. Simply logging in under the account, making changes, then logging out does not apply to this situation. A few changes will be remembered due to how Microsoft handles user profiles (even when they are only a member of the Guests group), but these are extremely limited. Having a guest account for the user account changes the way you must think about locking down access. It makes it very easy to cleanup when the user logs off, but much harder to lock down the desktop. To add to this increased difficulty, the system has different timing parameters between the very first user that logs onto the kiosk user account and any user after that. This has to be taking into consideration when using scripts that delay a timed number of seconds before beginning execution.

Backup, backup, backup

This cannot be stated enough. Backup the operating system if the tools are available. If the tools are not available, at least make sure to backup the security template as changes are made. It is very costly when three days have been spent securing a system, and one change causes a hiccup and everything is lost.

Keeping good documentation

This goes along with the above step. Always, ALWAYS keep good documentation. This cannot be emphasized enough! On week two of making changes, that binary change in the registry key may have made perfect sense, but trying to remember a few months later why the change was made may be very difficult. Some people have the fear that if everything is documented, someone else can come behind you and take your job. Well, if someone cannot come behind you and take over your work, you will create a situation where you cannot advance because you have become too vital to the mission. The person who was going to take over your job may now get the position you were destined for.

Windows 2000 and the RPC service

The importance of the service will be mentioned again. In the process of testing, this service was disabled. In Windows NT, disabling or removing this service did not cause many problems locally on the workstation. This was the assumption when disabling this service under Windows 2000. It turned out to definitely not be the case. Once this service was disabled, many other local services did not start. Local services were not much to worry about since the idea was to disable as

much as possible. The problems were noted when the system now took five times longer to boot and access the system. The only way to recover was to make changes to the security policy and re-apply it with the RPC service not enabled. The system was in such an unstable state that most of the Microsoft Management Console (MMC) plug-ins would not load. The system almost had to be scratched and rebuilt again. Luckily this was not the case, although a backup was available.

Are we done yet?

As mentioned earlier, this is only on piece of the pie. The system has been locked down, but the user still has many applications locally to play with. The idea of the kiosk is to only allow access to Internet Explorer. This means no WordPad, calculator, notepad, network browsing, etc. All these items have to be removed or locked away so the user cannot access them. How this is accomplished is dependent on the skills and choices made by the builder. The following are some quick suggestions for areas to pursue in further locking down the system.

Group Policies

Remember this fun area to work with in Active Directory? The local group policy is just as much fun. For those not familiar with group policies, it is an MMC snap-in like the "Security and Configuration Analysis" used in this document. The snap-in is simply called "Group Policy". One word of caution when make changes: always make backups along the way. There is nothing worse than locking down the system so tight it has to be reinstalled to get it back to a usable state. This statement is made from a lot of personal experience on the matter. Once the system has been fully secured using group policy changes, there are still some more things to accomplish. Group policy takes an enormous amount of work out of trying to find all the appropriate registry changes to lock down the system. Even with all the group policy configuration options, more areas not listed have to be locked down tighter. This can be performed using system startup and shutdown scripts and logon and logoff scripts. Once again, these areas are located within the group policy.

Registry entries

People familiar with Windows NT 4.0 will remember all the registry pokes when trying to lock down the workstation. Remember how many hours were spent exporting portions of the registry, using regedit and comparing the before and after changes using the file compare program (fc for those with bad memories)? SysDiff should also come to mind. Windows 2000 still has these resources available, although they work differently under Windows 2000. As Microsoft likes mentioning on all Q articles involving registry changes, make sure you can get back to the previous system state if the system becomes totally unusable. Here are some quick notes on the two most commonly used Microsoft tools mentioned above:

SysDiff

SysDiff is temperamental at best when run under Windows 2000. It usually fails out with a "destination file in use" error message near the end of comparing two system configurations. You may have better luck with it, but I have not so far. There are some better tools for the job, but SysDiff was the right price (i.e. free).

Regedit and file comparisons

The file compare program probably gave some administrators a quick panic attack when comparing regedit exports. Nothing like comparing two files and just getting one character per line for the entire comparison. The exported entries for regedit are now in the Unicode format. When comparing two registry exports, use the option "fc /u" and it will work without any problems. Exporting registry files still works just as well for Windows 2000 as it did for Windows NT. With Windows 2000 Professional based off Windows NT, many of the registry pokes that worked for NT work for Windows 2000 --- notice I said many and not all.

Custom Scripts

It will always benefit the developer to have some programming knowledge. The more languages the developer can program in, the better. The idea behind this is because each language excels in different areas. Unfortunately, it is very rare that one language does everything. Here is a quick rundown on three of the more commonly used scripting languages:

Batch file (command line) scripting

This type of scripting has been around forever. The problem is that batch file scripting is very limited. Another item to keep in mind is that executing batch file scripts throws up a command box that can easily be closed. Once the command box is closed, the script no longer executes.

VBScript – the basis of Windows Scripting Host (WSH)

I have to admit that the latest implementation of VBScript (version 5.6) does almost everything any administrator would need to accomplish. As a side note, for those people reading this that say "If it doesn't require a bash (#) on the first line, it's not a real scripting language", get back to your Linux system. This language is definitely worth the time to learn. Even better, you really do not need to buy any books to learn this language. Microsoft has an associated executable to VBScript that installs documentation on VBScript programming. There are examples in the documentation on about every command used in VBScript. For someone with very little VBScript knowledge, cutting and pasting examples works great as a learning tool. This was the primary language used for the modifications to the kiosk guest user account.

Perl

This language has been used for years on Unix systems. Someone finally realized a few years ago that Microsoft users were also interested in the language. Even the Windows NT Resource Kit comes with a Perl command line executable, although it is quite limited. The biggest problem with Perl is that most of the good stuff has to be added on separately via modules, which requires Perl to be installed on the system. If you plan to do a lot of programming in Perl, I would highly suggest purchasing the Perl Resource Kit. The main advantage is the ability to create Perl executables that can be run on any system without any programs besides the Perl compiled program.

This works great for workstation modifications that could not be performed via VBScript.

Internet Explorer execution in Kiosk mode

Ever heard of this option before in Internet Explorer? Neither had I before perusing TechNet for some help. To open Internet Explorer in kiosk mode, use the following options: "IEXPLORE –nohome –k http:<web site>". Internet Explorer will run and cover the entire screen (start bar and all). The problem is that there are still a lot of shortcut keys that can be used in this mode that will have to be disabled. If the user presses [CTRL]+[N], another window opens in non-kiosk mode. Microsoft insists this is how it was programmed to work; I tend to disagree. This was tested on the kiosk without the hotkeys and worked quite well, until one of the pages launched a separate login window that opened up as a normal Internet Explorer window. Another drawback is when the right mouse button click is disabled (as was performed on this kiosk image) the standard back, refresh and other buttons are not available. This means that the hot keys must be posted near the machine. This provided to be a quick reason to dwell more into locking down the workstation and using registry pokes to throw up Internet Explorer as a full screen (without kiosk mode). As always, test everything as much as possible.

Delete what is not needed in the Start menu and Quick Launch toolbar

Programs in the start menu such as calculator, imaging, etc. are auto-generated when the profile is first created. Scripting will have to be used to delete these directories and files. Remember to check for more files in the "All Users" directory. Keep in mind that some of the "All Users" directories are recreated on logon if they do not exist.

The files for the quick launch start bar are located in a hidden directory in the user profile. The location for the quick launch tool bar is: %userprofile%\Application Data\Microsoft\Internet Explorer\Quick Launch. Delete shortcuts not needed from this area, and copy any modified ones using scripts if needed.

Remove access to everything but the community web server

These kiosk computers should only be able to access the community web server. No general web surfing will be allowed. How do you accomplish this? Here is a big hint: routing. You will have to get the route to the community web server and push it manually, then blow away the default route on the machine. Remember to also add the DNS entry to the \WINNT\SYSTEM32\DRIVERS\HOSTS file since you will most likely also kill access to the DNS server. Make sure to test that there are no links required that spawn off to a related server, for example from www.community.net to server2.community.net. It is much more difficult for a user to access a web site if only an IP address can be used, and this can be limited by deleting routes. The best way to accomplish all this is via system startup scripts.

Summary

The focus of this document was the implementation of the Microsoft supplied high security template on a kiosk. This template combined with the MMC snap-in "Security Analysis and Configuration" provided a comprehensive and graphical interface to the security template. The template was analyzed against the current system, pertinent changes made to the default high security template, and finished by applying the modified template. Microsoft has done a very good job of creating a one-stop area for applying many security changes to a system in one swoop. The high security template used worked very well, and had very few areas for improvement. The modifications made to the template were mostly because of the function of the system. The purpose of the template is to secure a standard Windows 2000 Professional workstation; we used this template as a basis for a system with extremely limited kiosk access. The high security template would function well at its original purpose to lock down a workstation.

Developing a kiosk takes a lot of time and patience. This task was a full test of all the Microsoft knowledge I have amassed over the years. Applying the security template ended up being only a small portion of the work. I had hopes that the security template and group policies could accomplish everything, but as usual they fall just a few short. This was expected since Microsoft's intent for Windows 2000 Professional is to be accessed by users, not setup as a kiosk. Microsoft has come a long way on accomplishing this goal with the tools they provide. I was quite surprised how much the system could be locked down using the template and group policies.

Hopefully you finish reading this paper with an appreciation for all the work Microsoft has put into controlling the desktops with a minimal number of tools. Kiosks are one of the most difficult machines to create because security is so vital, and the high security template provided a good starting point. If ever in doubt, secure it. Throughout the development and testing, the underlying question was always how secure is secure? So now that you have read all this, go take a shot at creating your own kiosk!

Bibliography

Bragg, Roberta. *Windows 2000 Security*. Indianapolis: New Riders Publishing, 2001

Microsoft Corporation. "CTRL+N Starts New Instance of Internet Explorer in Kiosk Mode [Q258864]" 13 Sep. 2001. URL: http://support.microsoft.com/default.aspx?scid=kb;EN-US;q258864

Microsoft Corporation. "How to Use Kiosk Mode in Microsoft Internet Explorer [Q154780]" 10 Oct. 2001. URL: http://support.microsoft.com/default.aspx?scid=kb;EN-US;q154780

Microsoft Corporation. "Implementing Common Desktop Management Scenarios – White Paper" 26 Oct. 2000. URL:http://www.microsoft.com/windows2000/techinfo/howitworks/management/grouppolicy.asp

Microsoft Corporation. "Microsoft Full-Text Search Technologies – White Paper" 26 July 2001. URL: http://www.microsoft.com/sharepoint/techinfo/planning/SearchTechnologies.doc

Microsoft Corporation. "Restricting Information Available to Anonymous Logon Users [Q143474]" 8 Aug. 2001. URL: http://support.microsoft.com/default.aspx?scid=kb;EN-US;q143474

Microsoft Windows 2000 Professional Resource Kit. Redmond: Microsoft Press, 2000

Microsoft Windows 2000 Server Resource Kit. Redmond: Microsoft Press, 2000

Appendix

Kiosk.Inf – Security template file

```
[Unicode]
Unicode=yes
[Version]
signature="$CHICAGO$"
Revision=1
[Profile Description]
Description=Increases SecureWS Settings.  Restricts Power User and Terminal Server ACLs.
[System Access]
MinimumPasswordAge = 2
MaximumPasswordAge = 42
MinimumPasswordLength = 7
PasswordComplexity = 1
PasswordHistorySize = 24
LockoutBadCount = 3
ResetLockoutCount = 30
LockoutDuration = 30
RequireLogonToChangePassword = 0
NewAdministratorName = "admin"
NewGuestName = "no access"
ClearTextPassword = 0
[System Log]
MaximumLogSize = 4096
AuditLogRetentionPeriod = 0
RestrictGuestAccess = 1
[Security Log]
MaximumLogSize = 10240
AuditLogRetentionPeriod = 0
RestrictGuestAccess = 1
[Application Log]
MaximumLogSize = 4096
AuditLogRetentionPeriod = 0
RestrictGuestAccess = 1
[Event Audit]
AuditSystemEvents = 3
```

AuditLogonEvents = 3

AuditObjectAccess = 3

AuditPrivilegeUse = 3

AuditPolicyChange = 3

AuditAccountManage = 3

AuditProcessTracking = 0

AuditAccountLogon = 3

[Registry Values]

machine\system\currentcontrolset\services\netlogon\parameters\signsecurechannel=4,1

machine\system\currentcontrolset\services\netlogon\parameters\sealsecurechannel=4,1

machine\system\currentcontrolset\services\netlogon\parameters\requirestrongkey=4,1

machine\system\currentcontrolset\services\netlogon\parameters\requiresignorseal=4,1

machine\system\currentcontrolset\services\netlogon\parameters\disablepasswordchange=4,0

machine\system\currentcontrolset\services\lanmanworkstation\parameters\requiresecuritysignature=4,1

machine\system\currentcontrolset\services\lanmanworkstation\parameters\enablesecuritysignature=4,1

machine\system\currentcontrolset\services\lanmanworkstation\parameters\enableplaintextpassword=4,0

machine\system\currentcontrolset\services\lanmanserver\parameters\requiresecuritysignature=4,1

machine\system\currentcontrolset\services\lanmanserver\parameters\enablesecuritysignature=4,1

machine\system\currentcontrolset\services\lanmanserver\parameters\enableforcedlogoff=4,1

machine\system\currentcontrolset\services\lanmanserver\parameters\autodisconnect=4,15

machine\system\currentcontrolset\control\session manager\protectionmode=4,1

machine\system\currentcontrolset\control\session manager\memory management\clearpagefileatshutdown=4,1

machine\system\currentcontrolset\control\print\providers\lanman print services\servers\addprinterdrivers=4,1

machine\system\currentcontrolset\control\lsa\restrictanonymous=4,2

machine\system\currentcontrolset\control\lsa\lmcompatibilitylevel=4,5

machine\system\currentcontrolset\control\lsa\fullprivilegeauditing=3,0

machine\system\currentcontrolset\control\lsa\crashonauditfail=4,0

machine\system\currentcontrolset\control\lsa\auditbaseobjects=4,0

machine\software\microsoft\windows\currentversion\policies\system\legalnoticetext=1,WARNING: All use of this system and network activity is monitored. Logging into this system is understood as a consent to this monitoring. Any illegal actions performed on this terminal will result in prosecution to the full extent of the law. Click OK below to agree to the above access requirement.

machine\software\microsoft\windows\currentversion\policies\system\legalnoticecaption=1,Login message

machine\software\microsoft\windows\currentversion\policies\system\dontdisplaylastusername=4,1

machine\software\microsoft\windows\currentversion\policies\system\disablecad=4,0

machine\software\microsoft\windows nt\currentversion\winlogon\scremoveoption=1,1

machine\software\microsoft\windows nt\currentversion\winlogon\passwordexpirywarning=4,14

machine\software\microsoft\windows nt\currentversion\winlogon\cachedlogonscount=1,10

machine\software\microsoft\windows nt\currentversion\winlogon\allocatefloppies=1,0

machine\software\microsoft\windows nt\currentversion\winlogon\allocatedasd=1,0

machine\software\microsoft\windows nt\currentversion\winlogon\allocatecdroms=1,0

machine\software\microsoft\windows nt\currentversion\setup\recoveryconsole\setcommand=4,0

machine\software\microsoft\windows nt\currentversion\setup\recoveryconsole\securitylevel=4,0

machine\software\microsoft\non-driver signing\policy=3,0

machine\software\microsoft\driver signing\policy=3,1

[Privilege Rights]

senetworklogonright =

[Registry Keys]

1="machine\software", 2, "D:P(A;CI;GR;;;BU)(A;CI;GR;;;PU)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI;GA;;;CO)"

2="machine\software\classes", 2, "D:(A;CI;GR;;;WD)"

3="machine\software\microsoft\netdde", 2, "D:P(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI;GA;;;CO)"

4="machine\software\microsoft\protected storage system provider", 1, "D:AR"

5="machine\software\microsoft\secure", 2,
"D:P(A;CI;GR;;;BU)(A;CI;GR;;;PU)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI;GA;;;CO)"

6="machine\software\microsoft\systemcertificates", 2,
"D:P(A;CI;GR;;;BU)(A;CI;GR;;;PU)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI;GA;;;CO)"

7="machine\software\microsoft\windows nt\currentversion", 2, "D:(A;CI;GR;;;WD)"

8="machine\software\microsoft\windows nt\currentversion\accessibility", 2,
"D:P(A;CI;GR;;;BU)(A;CI;GR;;;PU)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI;GA;;;CO)"

9="machine\software\microsoft\windows nt\currentversion\aedebug", 2,
"D:P(A;CI;GR;;;BU)(A;CI;GR;;;PU)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI;GA;;;CO)"

a="machine\software\microsoft\windows nt\currentversion\asrcommands", 2,
"D:P(A;CI;GR;;;BU)(A;CI;GR;;;PU)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI;GA;;;CO)(A;CI;GRGWSD;;;BO)"

b="machine\software\microsoft\windows nt\currentversion\classes", 2,
"D:P(A;CI;GR;;;BU)(A;CI;GR;;;PU)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI;GA;;;CO)"

c="machine\software\microsoft\windows nt\currentversion\drivers32", 2,
"D:P(A;CI;GR;;;BU)(A;CI;GR;;;PU)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI;GA;;;CO)"

d="machine\software\microsoft\windows nt\currentversion\efs", 2,
"D:P(A;CI;GR;;;BU)(A;CI;GR;;;PU)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI;GA;;;CO)"

e="machine\software\microsoft\windows nt\currentversion\font drivers", 2,
"D:P(A;CI;GR;;;BU)(A;CI;GR;;;PU)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI;GA;;;CO)"

f="machine\software\microsoft\windows nt\currentversion\fontmapper", 2,
"D:P(A;CI;GR;;;BU)(A;CI;GR;;;PU)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI;GA;;;CO)"

10="machine\software\microsoft\windows nt\currentversion\image file execution options", 2,
"D:P(A;CI;GR;;;BU)(A;CI;GR;;;PU)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI;GA;;;CO)"

11="machine\software\microsoft\windows nt\currentversion\inifilemapping", 2,
"D:P(A;CI;GR;;;BU)(A;CI;GR;;;PU)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI;GA;;;CO)"

12="machine\software\microsoft\windows nt\currentversion\perflib", 2,
"D:P(A;CI;GR;;;IU)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI;GA;;;CO)"

13="machine\software\microsoft\windows nt\currentversion\perflib\009", 1, "D:AR"

14="machine\software\microsoft\windows nt\currentversion\profilelist", 2,
"D:P(A;CI;GR;;;BU)(A;CI;GR;;;PU)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI;GA;;;CO)"

15="machine\software\microsoft\windows nt\currentversion\secedit", 2,
"D:P(A;CI;GR;;;BU)(A;CI;GR;;;PU)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI;GA;;;CO)"

16="machine\software\microsoft\windows nt\currentversion\setup\recoveryconsole", 2,
"D:P(A;CI;GR;;;BU)(A;CI;GR;;;PU)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI;GA;;;CO)"

17="machine\software\microsoft\windows nt\currentversion\svchost", 2,
"D:P(A;CI;GR;;;BU)(A;CI;GR;;;PU)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI;GA;;;CO)"

18="machine\software\microsoft\windows nt\currentversion\time zones", 2,
"D:P(A;CI;GR;;;BU)(A;CI;GR;;;PU)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI;GA;;;CO)"

19="machine\software\microsoft\windows nt\currentversion\windows", 2,
"D:P(A;CI;GR;;;BU)(A;CI;GR;;;PU)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI;GA;;;CO)"

1a="machine\software\microsoft\windows nt\currentversion\winlogon", 2,
"D:P(A;CI;GR;;;BU)(A;CI;GR;;;PU)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI;GA;;;CO)"

1b="machine\software\microsoft\windows\currentversion\group policy", 1, "D:AR"

1c="machine\software\microsoft\windows\currentversion\installer", 1, "D:AR"

1d="machine\software\microsoft\windows\currentversion\policies", 1, "D:AR"

1e="machine\system", 2, "D:P(A;CI;GR;;;BU)(A;CI;GR;;;PU)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI;GA;;;CO)"

1f="machine\system\clone", 1, "D:AR"

20="machine\system\controlset001", 1, "D:AR"

21="machine\system\controlset002", 1, "D:AR"

22="machine\system\controlset003", 1, "D:AR"

23="machine\system\controlset004", 1, "D:AR"

24="machine\system\controlset005", 1, "D:AR"

25="machine\system\controlset006", 1, "D:AR"

26="machine\system\controlset007", 1, "D:AR"

27="machine\system\controlset008", 1, "D:AR"

28="machine\system\controlset009", 1, "D:AR"

29="machine\system\controlset010", 1, "D:AR"

2a="machine\system\currentcontrolset\control\computername", 2, "D:(A;CI;GR;;;WD)"

2b="machine\system\currentcontrolset\control\contentindex", 2, "D:(A;CI;GR;;;WD)"

2c="machine\system\currentcontrolset\control\keyboard layout", 2, "D:(A;CI;GR;;;WD)"

2d="machine\system\currentcontrolset\control\keyboard layouts", 2, "D:(A;CI;GR;;;WD)"

2e="machine\system\currentcontrolset\control\print\printers", 2, "D:(A;CI;GR;;;WD)"

2f="machine\system\currentcontrolset\control\productoptions", 2, "D:(A;CI;GR;;;WD)"

30="machine\system\currentcontrolset\control\securepipeservers\winreg", 2, "D:P(A;CI;GA;;;BA)(A;;GR;;;BO)"

31="machine\system\currentcontrolset\control\wmi\security", 2, "D:P(A;CI;GR;;;BA)(A;CI;GA;;;SY)(A;CI;GA;;;CO)"

32="machine\system\currentcontrolset\enum", 1, "D:AR"

33="machine\system\currentcontrolset\hardware profiles", 1, "D:AR"

34="machine\system\currentcontrolset\services\eventlog", 2, "D:(A;CI;GR;;;WD)"

35="machine\system\currentcontrolset\services\tcpip", 2, "D:(A;CI;GR;;;WD)"

36="users\.default", 2, "D:P(A;CI;GR;;;BU)(A;CI;GR;;;PU)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI;GA;;;CO)"

37="users\.default\software\microsoft\netdde", 2, "D:P(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI;GA;;;CO)"

38="users\.default\software\microsoft\protected storage system provider", 1, "D:AR"

[File Security]

1="c:\", 0, "D:AR(A;OICI;FA;;;LA)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)"

2="c:\autoexec.bat", 2, "D:P(A;;GRGX;;;BU)(A;;GRGX;;;PU)(A;;GA;;;BA)(A;;GA;;;SY)"

3="c:\boot.ini", 2, "D:P(A;;GRGX;;;PU)(A;;GA;;;BA)(A;;GA;;;SY)"

4="c:\config.sys", 2, "D:P(A;;GRGX;;;BU)(A;;GRGX;;;PU)(A;;GA;;;BA)(A;;GA;;;SY)"

5="c:\documents and settings", 0,
"D:AR(A;OICI;FA;;;BA)(A;OICI;0x1200a9;;;AU)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)"

6="c:\ntbootdd.sys", 2, "D:P(A;;GRGX;;;PU)(A;;GA;;;BA)(A;;GA;;;SY)"

7="c:\ntdetect.com", 2, "D:P(A;;GRGX;;;PU)(A;;GA;;;BA)(A;;GA;;;SY)"

8="c:\ntldr", 2, "D:P(A;;GRGX;;;PU)(A;;GA;;;BA)(A;;GA;;;SY)"

9="c:\program files", 2,
"D:P(A;CIOI;GRGX;;;BU)(A;CIOI;GRGX;;;PU)(A;CIOI;GA;;;BA)(A;CIOI;GA;;;SY)(A;CIOI;GA;;;CO)"

a="c:\winnt", 2,
"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;0x1200a9;;;PU)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)"

b="c:\winnt\addins", 2,
"D:P(A;CIOI;GRGX;;;BU)(A;CIOI;GRGX;;;PU)(A;CIOI;GA;;;BA)(A;CIOI;GA;;;SY)(A;CIOI;GA;;;CO)"

c="c:\winnt\connection wizard", 2,
"D:P(A;CIOI;GRGX;;;BU)(A;CIOI;GRGX;;;PU)(A;CIOI;GA;;;BA)(A;CIOI;GA;;;SY)(A;CIOI;GA;;;CO)"

d="c:\winnt\csc", 1, "D:AR"

e="c:\winnt\debug", 1, "D:AR"

f="c:\winnt\driver cache", 2,
"D:P(A;CIOI;GRGX;;;BU)(A;CIOI;GRGX;;;PU)(A;CIOI;GA;;;BA)(A;CIOI;GA;;;SY)(A;CIOI;GA;;;CO)"

10="c:\winnt\explorer.exe", 2, "D:(A;;GRGX;;;WD)"

11="c:\winnt\java", 2,
"D:P(A;CIOI;GRGX;;;BU)(A;CIOI;GRGX;;;PU)(A;CIOI;GA;;;BA)(A;CIOI;GA;;;SY)(A;CIOI;GA;;;CO)"

12="c:\winnt\msagent", 2,
"D:P(A;CIOI;GRGX;;;BU)(A;CIOI;GRGX;;;PU)(A;CIOI;GA;;;BA)(A;CIOI;GA;;;SY)(A;CIOI;GA;;;CO)"

13="c:\winnt\offline pages", 1, "D:AR"

14="c:\winnt\profiles", 1, "D:AR"

15="c:\winnt\registration", 1, "D:AR"

16="c:\winnt\repair", 2,
"D:P(A;CI;GRGX;;;BU)(A;CI;GRGX;;;PU)(A;CIOI;GA;;;BA)(A;CIOI;GA;;;SY)(A;CIOI;GA;;;CO)"

17="c:\winnt\security", 2,
"D:P(A;CIOI;GRGX;;;BU)(A;CIOI;GRGX;;;PU)(A;CIOI;GA;;;BA)(A;CIOI;GA;;;SY)(A;CIOI;GA;;;CO)"

```
18="c:\winnt\speech", 2,
"D:P(A;CIOI;GRGX;;;BU)(A;CIOI;GRGX;;;PU)(A;CIOI;GA;;;BA)(A;CIOI;GA;;;SY)(A;CIOI;GA;;;CO)"

19="c:\winnt\system32", 2,
"D:P(A;CIOI;GRGX;;;BU)(A;CIOI;GRGX;;;PU)(A;CIOI;GA;;;BA)(A;CIOI;GA;;;SY)(A;CIOI;GA;;;CO)(A;CIOI;GRGX;;
;WD)"

1a="c:\winnt\system32\appmgmt", 1, "D:AR"

1b="c:\winnt\system32\catroot", 2,
"D:P(A;CIOI;GRGX;;;BU)(A;CIOI;GRGX;;;PU)(A;CIOI;GA;;;BA)(A;CIOI;GA;;;SY)(A;CIOI;GA;;;CO)"

1c="c:\winnt\system32\config", 2,
"D:P(A;CI;GRGX;;;BU)(A;CI;GRGX;;;PU)(A;CIOI;GA;;;BA)(A;CIOI;GA;;;SY)(A;CIOI;GA;;;CO)"

1d="c:\winnt\system32\dhcp", 2,
"D:P(A;CIOI;GRGX;;;BU)(A;CIOI;GRGX;;;PU)(A;CIOI;GA;;;BA)(A;CIOI;GA;;;SY)(A;CIOI;GA;;;CO)"

1e="c:\winnt\system32\dllcache", 2, "D:P(A;CIOI;GA;;;BA)(A;CIOI;GA;;;SY)(A;CIOI;GA;;;CO)"

1f="c:\winnt\system32\drivers", 2,
"D:P(A;CIOI;GRGX;;;BU)(A;CIOI;GRGX;;;PU)(A;CIOI;GA;;;BA)(A;CIOI;GA;;;SY)(A;CIOI;GA;;;CO)"

20="c:\winnt\system32\dtclog", 1, "D:AR"

21="c:\winnt\system32\grouppolicy", 1, "D:AR"

22="c:\winnt\system32\ias", 2, "D:P(A;CIOI;GA;;;BA)(A;CIOI;GA;;;SY)(A;CIOI;GA;;;CO)"

23="c:\winnt\system32\mui", 2,
"D:P(A;CIOI;GRGX;;;BU)(A;CIOI;GRGX;;;PU)(A;CIOI;GA;;;BA)(A;CIOI;GA;;;SY)(A;CIOI;GA;;;CO)"

24="c:\winnt\system32\ntmsdata", 1, "D:AR"

25="c:\winnt\system32\reinstallbackups", 1,
"D:P(A;CIOI;GRGX;;;BU)(A;CIOI;GRGX;;;PU)(A;CIOI;GA;;;BA)(A;CIOI;GA;;;SY)(A;CIOI;GA;;;CO)"

26="c:\winnt\system32\repl", 1,
"D:P(A;CIOI;GRGX;;;BU)(A;CIOI;GRGX;;;PU)(A;CIOI;GA;;;BA)(A;CIOI;GA;;;SY)(A;CIOI;GA;;;CO)"

27="c:\winnt\system32\repl\export", 1, "D:(A;CIOI;GRGWGXSD;;;RE)"

28="c:\winnt\system32\repl\import", 1, "D:(A;CIOI;GRGWGXSD;;;RE)"

29="c:\winnt\system32\setup", 1, "D:AR"

2a="c:\winnt\system32\shellext", 2,
"D:P(A;CIOI;GRGX;;;BU)(A;CIOI;GRGX;;;PU)(A;CIOI;GA;;;BA)(A;CIOI;GA;;;SY)(A;CIOI;GA;;;CO)"

2b="c:\winnt\system32\spool\printers", 1,
"D:P(A;CI;GRGX;;;BU)(A;CIOI;GRGX;;;PU)(A;CIOI;GA;;;BA)(A;CIOI;GA;;;SY)(A;CIOI;GA;;;CO)"

2c="c:\winnt\system32\wbem", 2,
"D:P(A;CIOI;GRGX;;;BU)(A;CIOI;GRGX;;;PU)(A;CIOI;GA;;;BA)(A;CIOI;GA;;;SY)(A;CIOI;GA;;;CO)"

2d="c:\winnt\system32\wbem\mof", 2,
"D:P(A;CIOI;GRGX;;;BU)(A;CIOI;GRGX;;;PU)(A;CIOI;GA;;;BA)(A;CIOI;GA;;;SY)(A;CIOI;GA;;;CO)"

2e="c:\winnt\tasks", 1, "D:AR"

2f="c:\winnt\temp", 2,
"D:P(A;CI;0x100026;;;BU)(A;CI;0x100026;;;PU)(A;CIOI;GA;;;BA)(A;CIOI;GA;;;SY)(A;CIOI;GA;;;CO)"

30="c:\winnt\twain_32", 2,
"D:P(A;CIOI;GRGX;;;BU)(A;CIOI;GRGX;;;PU)(A;CIOI;GA;;;BA)(A;CIOI;GA;;;SY)(A;CIOI;GA;;;CO)"

31="c:\winnt\web", 2,
"D:P(A;CIOI;GRGX;;;BU)(A;CIOI;GRGX;;;PU)(A;CIOI;GA;;;BA)(A;CIOI;GA;;;SY)(A;CIOI;GA;;;CO)"
```

[Service General Setting]

1="appmgmt", 4,
"D:(A;OICI;CCLCSWLORC;;;WD)(A;OICI;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;OICI;CCDCLCSWLORC;;;PU)(A;OICI;CCLCSWRPLO;;;IU)(A;OICI;CCLCSWRPLO;;;BU)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"

2="cisvc", 4,
"D:(A;;CCLCSWRPWPDTLOCRRC;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"

3="clipsrv", 4,
"D:(A;OICI;CCLCSWLORC;;;WD)(A;OICI;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;OICI;CCDCLCSWLORC;;;PU)(A;OICI;CCLCSWRPLO;;;IU)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"

4="dhcp", 4,
"D:(A;;CCLCSWRPWPDTLOCRRC;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"

5="fax", 4,
"D:(A;;CCLCSWRPWPDTLOCRRC;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;LCRP;;;WD)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"

6="lmhosts", 4,
"D:(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPLOCRRC;;;PU)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWRPWPDTLOCRRC;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"

7="mnmsrvc", 4,
"D:(A;;CCLCSWRPWPDTLOCRRC;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"

8="rasauto", 4,
"D:(A;;CCLCSWRPWPDTLOCRRC;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"

9="rasman", 4,
"D:(A;;CCLCSWRPLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"

a="remoteregistry", 4,
"D:(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPLOCRRC;;;PU)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWRPWPDTLOCRRC;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"

b="schedule", 4,
"D:(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPLOCRRC;;;PU)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWRPWPDTLOCRRC;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"

c="sharedaccess", 4,
"D:(A;;CCLCSWRPWPDTLOCRRC;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"

d="tapisrv", 4,
"D:(A;OICI;CCLCSWLORC;;;WD)(A;OICI;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;OICI;CCLCSWLORC;;;PU)(A;OICI;CCLCSWRPLO;;;IU)(A;OICI;CCLCSWRPLO;;;BU)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"

e="tlntsvr", 4,
"D:(A;;CCLCSWRPWPDTLOCRRC;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"

Last Updated: July 21st, 2017

Upcoming Training

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 13, 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 Cyber Defense Initiative 2017	**Washington, DC**	**Dec 12, 2017 - Dec 19, 2017**	**Live Event**
SANS Southern California- Anaheim 2018	**Anaheim, CA**	**Feb 12, 2018 - Feb 17, 2018**	**Live Event**
SANS OnDemand	**Online**	**Anytime**	**Self Paced**
SANS SelfStudy	**Books & MP3s Only**	**Anytime**	**Self Paced**