Global Information Assurance Certification Paper

The NSA W2K Workstation Template

By
Brian Stewart
GCWN Practical Assignment v.3.1 (Option 2)
October 9th 2002

Table of contents:

Abstract

This paper is a case study in the selection, application and testing of a Windows 2000 Professional Security Template. This document will address a project by a fictional international company to deploy several kiosk systems in a varied corporate environment. The Template to be discussed in this document is the Windows 2000 Workstation template provided by the National Security Administration of the United States of America.

There are many steps to building a kiosk system. This paper will primarily focus on the process of building a kiosk system utilizing the NSA Workstation Template. Because of this there will be many assumptions made due to factors outside the scope of this paper. Where appropriate to understand the security of the system supplementary explanations will be provided for these decisions. Other external factors including firewalls and network connectivity may be briefly discussed but are better left to be covered in other papers. Where appropriate, references or hyperlinks to additional external information will be provided for topics outside the scope of this paper.

The Challenge

The IT group of our fictional international company has been tasked with building a number of kiosk workstations. These workstations are to allow internal and external users access to the Internet. Several of these stations will be located in uncontrolled public areas of corporate office buildings. Additionally a number of "cyber-cafes" will be built. This will include one in the training center to be used by both internal and external personnel during training events and conferences. These workstations will allow easy connectivity to the Internet for visitors. They will also provide Intranet access to internal employees while away from their offices.

The description of the completed systems provided by the management team was "simple". The kiosk stations are to allow any user to access the Internet in order to browse websites using either insecure (http) or secure (https) services as necessary. Any user will be allowed to check e-mail using web based portal applications such as Outlook Web Access or iPlanet or by using Internet mail services such as Hotmail or Yahoo mail. In addition, internal users will be allowed to browse the corporate intranet and check their internal e-mail.

These "simple" requirements present a number of security issues that must be considered in this deployment and those will be discussed in greater detail later in this document. The system must be protected from both local and remote compromise. A method must be provided to restrict the access of users from outside the company to external resources only. There must be assurance that no leakage of information is allowed from one user to another to protect users privacy. Insure that the systems are not used for inappropriate activities in order to protect the company from liability.

The Plan

The process used by many IT groups to deploy a number of systems in a short amount of time is to create a deployment image. First a single system is built and configured according to the final required specifications. An image is made of the system and then copied to the remaining systems to be deployed. As all of the initial systems can be ordered from the same vendor, and should include the same hardware, this process will work very well in this project for the initial deployment.

As most everyone is more than well aware, the default hardware used by most vendors changes every few months. New processors, controllers, video cards, network cards, sound cards and other devices are released on the market almost daily. Each of these devices requires specialized drivers to be installed on the system to operate properly. As experience has taught many in the IT field, the images of systems that are created during a large deployment will typically perform best on the single hardware platform on which they were originally built. While it may be possible to adapt images to new hardware devices this can often cause issues with drivers and libraries causing the completed system to become unstable. In most cases it is preferred to simply rebuild the system on the new hardware.

This causes a potential problem for future deployments of the kiosk project. The images being created now may not work on the systems that will be purchased next year, as they will most assuredly not have the same hardware specifications. In order to try and save some time when building the systems next year, the configuration of the base system will be well documented as it is built. This will allow the process to be repeated for any new hardware platforms purchased later in order to create a new deployment image utilizing a minimum of time and resources.

In order to secure any Windows 2000 Professional installation a number of steps are required. It is often necessary to edit the registry of the system in order to change required settings due to the lack of Graphical User Interfaces to control many of the functions of the system. In order to reduce the number of individual changes required and to insure that the changes are consistent in each build, a standard template will be used during the creation of each base image. This template will be selected following further review of the system requirements. This template will then be applied and tested for both security and functionality. Following testing of the template, a final deployment image will be made for the initial deployment.

Description of System

Role of the System

The first step in any project is to define the specific role and requirements of the system in order to select the best hardware, software and security configuration to provide the best solution. As stated before, management has defined the basic role of the systems with only a few simple statements.

- The kiosk stations are to allow any user to access the Internet in order to browse websites using either insecure (http) or secure (https) services as necessary.
- Any user will be allowed to check e-mail using web based portal applications such as Outlook Web Access or iPlanet or by using Internet mail services such as Hotmail or Yahoo mail.
- Internal users will be allowed to browse the corporate intranet and check their internal e-mail.

Hardware Specifications

To fulfill the requirements of the Internet kiosks project the systems will be based on a standard Personal Computer platform. The specific hardware specifications of the systems will vary during the project based on the procurement process in place at the time. Each system should meet the minimum specifications as follows.

Processor:	Pentium II
Memory:	128MB
Hard disk:	6 Gig
Video:	8MB
CD-ROM:	24x
Network Card:	Any Ethernet Adapter

For this deployment the following hardware platform will be used.

Dell Optiplex™ Desktop Computer

Processor:	Celeron 1.20/100GHz, 256K Cache
Memory:	128MB
Hard disk:	20 Gig
Video:	16MB
CD-ROM:	52x
Network Card:	Any Ethernet Adapter

Software Specifications

As this system will primarily be performing the task of a workstation the decision has been made to use Windows 2000 Professional as the operating system with Internet Explorer as the web browser.

The decision to use Windows 2000 was made for a number of reasons. The Windows operating system desktop and Internet Explorer web browser software are familiar to most everyone. This makes the final product user-friendly to the majority of users. The Internet Explorer web browser is also compatible with essentially every website and portal providing benefits that no other operating system could.

In addition to the Internet Explorer browser, it will be necessary to install a number of browser plug-in applications to provide a complete web experience for the users. These will include Adobe Acrobat Reader, Macromedia Flash and Shockwave players and Windows media player. Adding these programs will allow users to view the widest possible number of websites as they were intended.

The kiosk systems will be configured to use the new "Automatic Update" utility provided by Microsoft. This utility allows a system to automatically check the "Windows Update" website for critical service packs and hotfixes, download the necessary files and then install the updates. This decreases the amount of administration required in order to keep a system patches current.

The "Automatic Update" utility can be configured in a number of ways. The tool can simply check for updates then prompt the user to download and install them. It can automatically download the required updates but then wait for user confirmation prior to installation. Or finally it can be configured to operate completely automatically where it will check for updates, download them and install them without any user interaction.

Virus scanning software will be installed on the systems to protect them from malware that may be downloaded from the Internet or embedded in websites utilizing java or ActiveX scripts. In this deployment, Norton Antivirus 2002 will be used based on it's ability to provide the services required for this deployment. It's auto-protect and script-blocking features provide the necessary scanning solution for the kiosk. Norton AntiVirus has the ability to perform self-maintenance by updating not only the virus definitions but also the program automatically. The virus scanner will be configured to automatically update its definition files as they become available. The system hard disks will also be scanned on a weekly basis.

No other software will be loaded on the system. Most applications included with Windows 2000 Professional will not be installed during the initial build of the kiosk system. Reducing the number of software packages loaded on the system will reduce the opportunity for security vulnerabilities in unneeded applications to affect the security of the final system.

Security Requirements

In determining the security requirements of a kiosk system, it is important to recognize the latent risks involved in such a system. An easy method of determining the risks involved is to assess each system requirements potential weaknesses.

The primary requirement of a kiosk is that it has to be publicly accessible to anyone! Therefore the system must first and foremost be protected from physical theft. Several of the kiosk systems are to be placed in public areas. In this type of environment, the decision was made to lock the CPU in an enclosure mounted to a solid surface. This will restrict access to the device, the cable connections and most importantly to the CD and floppy drives. This eliminates theft of the components including the keyboard and mouse, as they cannot be disconnected from the CPU. It prevents the installation of hardware keystroke logging systems that could be used to steal usernames and passwords. It also restricts access to the CD and floppy drives eliminating the ability to use bootable media to circumnavigate the protections of the NTFS file system and access the hard disk. Finally, the monitors will be secured using cable locks to a solid structure. Security cameras will be installed to monitor the areas where the kiosk systems are located. This will provide evidence should criminal prosecution of a theft be necessary.

As users from outside the organization will use the systems, the decision was immediately made that the systems would not be allowed to connect directly to the corporate Local Area Networks. Supplementary telecommunications facilities will be acquired in order to connect the kiosks directly to the Internet using a broadband Internet connection. These facilities will consist of either a DSL or Cable modem connection to the Internet. These are to be provided by local resources at each site.

Having these systems connected directly to the Internet created an additional requirement that the systems be protected from external access. A firewall solution was developed using a NetScreen™ Stateful Inspection firewall and Network Address Translation to restrict all external access to the kiosk network. Furthermore the inherent filtering capabilities of the Windows 2000 operating system can be used to provide additional protection. A virus scanning software suite, discussed in the previous section, will also be installed to protect against viral threats and other malware.

The kiosk system is to provide access to the Internet for any user. This requires that a user be allowed access to the system without a username or password. A “default” or “kiosk” user account will have to be created to allow system access. This user account cannot require a password to be entered but can use a blank password. On an ordinary workstation there would be a limited amount of protection provided with the use of a username and password to gain access.

Due to the inability to prevent access to a kiosk system, the level of access that users are provided to the system must be tightly controlled. A user must not be allowed to run ANY applications other than the Internet Explorer browser, modify any of the system settings, install software, save files from the internet or restart the system. Users will also be prevented from viewing or modifying any of the log files stored on the system. By preventing these actions the system can be protected from a local user. Users will also be prevented from performing any inappropriate actions. These would include using the kiosk system to attempt to gain unauthorized access to another system. To assist with this many applications typically used to connect to remote systems such as FTP, TFTP and telnet will be disabled for the kiosk user.

The only remaining risk is that users may potentially view objectionable websites using the kiosk systems. To mitigate this risk, a content management system would be required to filter objectionable traffic. This is currently outside the scope of concern for this project.

Internal users must be allowed to connect to the Corporate Intranet and e-mail. This requires that there be a method of distinguishing internal users. In order to simplify the kiosk system, it was decided not to attempt a VPN solution. This would have added additional software to the system and created the necessity to insure that the user logged out of the VPN client. Instead it was decided to use a web portal solution that was implemented at the corporate headquarters to provide access from employees to the Intranet and internal e-mail systems. By using a web portal, users can easily log onto systems on the internal network. The connections will also be automatically terminated when the users close the web browser.

In order to protect the privacy of the kiosk users, the session information normally stored on the system must be protected. The kiosk system must not allow any of the typical information from a users session to be stored on the system. Much of this configuration will involve the Internet Explorer browser, as it must be configured not to store any information from sites visited in the cache files. The Internet history log of previously visited sites must be disabled. The permanent storage of Cookie files must be disabled in order to prevent the accidental storage of user credentials that could carryover from one users session to another.

This narrative assessment of security requirements will guide the process of building and configuring the Windows 2000 Professional system throughout the remainder of this project.

Template Selection

The security requirements previously determined require that the kiosk systems be as restricted as possible from both local and remote access. It is necessary to select a template that would restrict the most settings possible. In addition the

selection was rather restricted given that there are not an abundant number of templates available from reliable sources for the Windows 2000 Professional operating system.

For this project, the National Security Agency Windows 2000 Workstation template was chosen due to it's highly restrictive nature. Many of the settings in the NSA template are based upon the Microsoft hisecws.inf template. The NSA has provided security advice on the configuration of Unix, Microsoft and Cisco routers for a number of years and has become a highly respected source for security baselines. The NSA modified the base Microsoft template to add additional security settings based on its vast experience in building secure systems.

Despite the amount of work that has gone into the NSA Workstation template, it is unlikely that any template will be fully capable of providing the proper level of restrictions that are required for the kiosks being developed. Following the testing phase of this project it is expected that a number of enhancements will need to be made to the template prior to final deployment. The modified template can then be used during future development activities. It is also expected that there will be a number of security requirements that a security template will be incapable of providing. These will be resolved using a Group policy applied to the local computer.

Security Settings

The National Security Agency Windows 2000 Workstation Template provides for a number of security setting modifications to better protect a system from potential compromises. These settings allow the rapid and consistent configuration and analysis of a number of security areas as are specified by the Microsoft Security Template management interface including:

- Account Policies
- Local Policies
- Event Log
- Restricted Groups
- System Services
- Registry
- File System

Within each of these areas are a number of individual modifications to be applied to the system by the NSA security template. Each of these areas includes a number of system modifications that are of particular interest to engineers configuring a system being used as a Public kiosk. These modifications will be discussed by security area as defined by Microsoft. In order to avoid excessive duplication of the NSA guideline, only the benefits from each area that are relevant to the kiosk project and their significance will be discussed. For more detailed information on other settings modified by the template see the NSA

Account Policies

There are a number of modifications made by the NSA template to the default computer settings. This section includes three subsections; password policy, account lockout policy and the kerberos policy. Changes to the password policy provide for stronger passwords using a number of techniques. Passwords are configured to expire after 90 days. Password history is enforced to prevent users from using the same password repeatedly. Passwords must be a minimum of 1 day old to prevent a user changing a password repeatedly to defeat the password history feature. The passwords for the system are also required to be at least 12 characters in length. Each of these settings help to increasing the security of the system by making passwords harder to steal, guess or extract with a password cracking utility.

Changes to the account lockout policy provide for the locking of accounts when an invalid password is entered three times. After locking an account there is a 15-minute delay before the account is unlocked. The policies help to prevent brute force password guessing.

Changes to the kerberos policy modify the "kerberos logon enforcement" and "service ticket properties". Kerberos is only available for use on systems connected to a Windows 2000 Active Directory Domain! As this is a standalone system, these policies will not be defined.

Local Policies

The local policy settings modified by the NSA security template include changes to the auditing policy; user rights assignment and security options. Many of these changes are directly relevant to the kiosk environment.

Auditing should be enabled on every system. Auditing provides a method of maintaining logs of information detailing events that have taken place on the system. Windows 2000 Professional has all auditing disabled by default so it is necessary to configure any desired logging. The security template modifies the audit policy to enable the auditing of successful and failed logon events, account modification, system events, and policy changes. Although the security template enables the auditing of failed object access, it will require that the auditing properties of each object be modified before any logs are created. The NSA template also provides the ability to audit when a user performs privileged tasks. These tasks include adding users, performing backup and restore operations. This logging is useful to monitor when someone may be performing administrative tasks inappropriately. This is often a sign that a system has been compromised.

The user rights assignment policy section allows the limitation of specific actions to specified users. This can prevent users from performing tasks that should be reserved for administrators. These rights include logging into the system both locally and remotely. Access to the system resources can be limited for both local and remote users. The abilities to shutdown the system, take ownership of files and change the system time are also able to be limited.

The NSA template is very restrictive in that most rights are restricted to the Administrator. The only exceptions to this policy are that users can log on both locally and remotely, removed the system from the docking station and shutdown the system. These settings prevent users from modifying security logs, loading or unloading device drivers or taking ownership of files.

Security Options allow the modification of registry settings without requiring the use of the registry editor. Directly editing the registry can potentially harm the system due to unexpected results from editing the registry. The NSA template modifies the values of a number of registry keys and adds additional security options to modify keys not included in the default Microsoft settings. The most important changes in this section restrict anonymous remote connections. This prevents connection to the system using the "Null User" account. The template also sets the LAN manager authentication level to use only NTLMv2 and refuse LM & NTLM. This setting increases the difficulty in "cracking" passwords on a windows system or network by using tools such as L0phtCrack or John the ripper.

Event Log

The NSA security template provides for the configuration of several logging options. The maximum log size is set to the maximum value to gather as much data as possible. Guest users are restricted from viewing the Event logs for applications, security or the system. Logs are required to be manually cleared from the system insuring that the logs are not automatically destroyed. The system is configured to automatically shutdown when the log file is full.

These settings provide for the protection of the system and the preservation of the logs following a major event. They will insure that guests have no access to the logs. These modifications will also insure that the system will shutdown when the logs are full and require the administrator to clear the logs before the system can resume normal operations.

Restricted Groups

The use of restricted groups allows the administrator to control the membership of groups. The NSA security template provides for only the power users group and restricts the group to no members. The administrator of the system must modify the template prior to use due to the varying groups and users found on different systems.

System Services

This section allows for the configuration of system services such as network and file services. The system services sections provides for extremely granular control of services. Each service can be set to automatic, manual or disabled status when the system boots. The permissions of each service can also be configured to permit or deny users the ability to modify the status of a service. This will prevent a user from starting or stopping a critical service. Due to the varying service requirements, of systems the administrator must define this section before the template is applied.

Registry

This section of the security template provides for the modification of the permissions on a number of critical registry settings. This can prevent the unauthorized modification of registry settings by users other than the administrator.

File System

Windows 2000 provides for the ability to manage the file permissions of the NTFS file system using a security template. The NSA template reduces the privileges of the majority of common drives directories and files found on a system. The affected objects include the %ProgramFiles% and %SystemDirectory% directories and the %systemdrive%\boot.ini file containing the system boot information. The settings protect the system from unauthorized access to critical system files and folders.

Application, Testing and Evaluation

Building the Initial Windows 2000 Professional system

Prior to Applying the NSA Windows 2000 Template it is important to insure that the Windows operating system has been properly installed. It is also important to confirm that any unnecessary applications have been fully removed from the system. These are removed in order to prevent any of these non-essential applications becoming a vulnerability to the system if a problem is found at some point in the future. This also reduces the number of patches that must be installed on the system keeping maintenance at a minimum. This should be a common practice when building any system. The steps taken while securing the kiosk base installation are described in the following section.

Windows 2000 Professional Installation

A 4Gigabite primary partition was created on the system to act as the system drive. This should allow sufficient room to install all necessary applications and any future upgrades required during the usable life of the equipment. The partition was formatted using the NTFS file system to provide file and folder access controls. Windows 2000 Professional was installed into the directory of c:/win instead of the default of c:/winnt in order to provided some “security by

obscurity" by denying an attacker the knowledge of the exact directory structure of the system.

The following steps had little effect on the security of the system but are described to assist while replicating the system configuration. The system local settings were set to US as the system uses a US keyboard. The Name and Organizational information for the system were set to "kiosk" for this initial system. The Computer name of the system was set to "kiosk". A "hard" password was selected for the administrator account. In the network wizard "Home Use" and "Users must log in" are selected.

Drivers were installed for the video, network and audio cards. As the system used to build the image did not have drivers available on the Windows 2000 Professional CD. Instead, the drivers were installed from a CD provided by the hardware vendor.

Applying Service Packs and Hotfixes

Installing the base Windows 2000 Professional operating system was only the first step to building a secure system. The next step was to connect the system to a protected network in order to use the Microsoft "Windows Update" website. The "Windows Update" site was able to scan the system for any missing service packs that were required by the system. The first package downloaded was Windows 2000 Professional Service Pack III. This package had to be installed independently of all other packages and required the system to be rebooted following the installation.

After rebooting the system, the "Windows Update" site was again used to scan the system. As the majority of the required hotfixes were related to the Internet Explorer web browser, it was decided to update the system to Internet Explorer version 6.0 Service Pack 1. This eliminated a number of know issues with earlier versions of the program and will provide the most flexibility in relation to future changes to the system. Again the update package had to be installed independently of the remaining packages and required the system to be rebooted before continuing.

As Windows 2000 Professional has been available for some time a number of other hotfixes and updates were required. Each of these was responsible for patching known security vulnerabilities. The remaining required security updates suggested by the "Windows Update" website were installed on the system. At the time the system was built, there were 8 updates required. As most anyone in the security field is aware, new vulnerabilities are discovered and patches are released daily so your mileage may vary. The patches installed for this system include the following:

Q329077 – Flaw in Microsoft VM JDBC Classes
Q324096 - Buffer Overrun in SmartHTML Interpreter

Q323172 - Print Flaw in Certificate Enrollment Control
Q326830 - Unchecked Buffer in Network Share Provider
Q326886 - Flaw in Network Connection Manager
Q324380 - Cryptographic Flaw in RDP Protocol
Q323255 - Unchecked buffer in HTML
Security Update February 13th 2002 (MSXML 3.0)

After all the necessary updates were installed, it was necessary to configure the Automatic Update service. The service was installed as a part of the installation of the Windows 2000 Professional Service Pack 3. The service was configured to automatically check for updates, download the necessary files and install the updates on everyday of the week at 6AM. Using the Automatic update service will drastically decrease the amount of administration required on the systems in order to keep patches current. This should also reduce the potential for operating system and software vulnerabilities to affect the operation of the kiosks.

System Hardening

At this point, the operating system installation is complete and all the necessary patches have been installed. Several steps will now be taken to further harden the system prior to the application of the security template. First, the Administrator account is renamed and the default description are changed to protect the account. As this system is available to the public, it was decided to decrease the chance of someone guessing the administrative password by also changing the username to a name other than the default of "administrator". The "guest" account was also renamed, the default description was changed and the account left disabled.

To add a little paranoia to the system a new account was created called administrator. The account was added to the kiosk users group. The password was set to a nearly impossible string. Then the account was disabled. By adding this account it is possible to see when someone is trying to access the "administrator" account and log the activity. This will provide the real administrators with a warning that someone is trying to access the system.

Finally, a "kiosk" account was created. No password was defined for this account. The password was set to never expire. This account will allow access for normal users who cannot be expected to know a password in order to gain access to the system. A new group was created called "kiosk users". The "kiosk" user was added to this group. This will simplify making changes to permissions and allow flexibility for future added requirements.

Using the computer manager disk administrator tool, a second 2GB partition was created on the hard disk. This partition was formatted using the NTFS file system to provide Access control list protections. The CD-ROM drive letter was

changed to “X”. Again this was done primarily to provide some “security by obscurity” by denying knowledge of the basic system structure.

The system memory paging file settings were modified to store the paging file on the new partition with a minimum and maximum size setting of 384 MB. By setting the file size minimum and maximum to equal the paging file, it is prevented from expanding and contracting on the hard disk. This is becoming a more common practice as it stops the system from overwriting “free space” on the disk with virtual memory contents as the size of the paging file increases. This is primarily useful in the event that a forensic analysis of the hard disk must be performed. This step could potentially allow the recovery of deleted data that might have been overwritten had the paging file been allowed to contract and expand.

Next, the default networking settings were modified to remove all unnecessary bindings. Both the “File and Print Sharing for Microsoft Networks” and the ”Client for Microsoft Networks” bindings were uninstalled from the system. The removal of these bindings stopped several services including: Browser, Server, Workstation and Messenger. With these services removed from the system, it is no longer possible for a user to create local shares or to map drives to shares on another system. In a typical Windows network this may present a problem, but for the very limited environment that the kiosk will be used in, this configuration provides for extremely good protection. Finally, the TCP/IP properties “Advanced” section “Wins” configuration tab was modified to completely disable support for NetBios.

Several changes were made to the system at this time to prevent it from being locally exploited or being used to attack remote systems. The NTFS permissions of the executable files for telnet, FTP, TFTP command, the Microsoft Management Console (mmc) and cmd were modified. This will prevent their use by any user in the “kiosk user” group. For a paranoid security practitioner, the best solution would have been to remove these files from the system. Unfortunately, this is not a viable option for a couple of reasons. The first being that the Windows file protection feature will replace the files immediately after their being deleted. The second reason being that the files will be replaced with the install of the next service pack. In the future these changes will be added to the kiosk security template.

Software Installation

Norton Antivirus 2002 was installed on the system. Following the installation, it was necessary to run the “LiveUpdate” utility a number of times to retrieve the latest versions of the virus software and to update the virus definitions. After the system files were brought up to date, the virus scanner was configured to automatically check for new virus definition and software updates on a weekly basis. The application will then scan the entire system for viruses immediately following the updates.

The protection features of Norton Anti-virus providing auto-protect and script-blocking functionality are enabled by default. These will prevent users from inadvertently or maliciously downloading malware, Trojans, virus and even damaging scripts from the Internet to the local system. The e-mail protection feature was disabled since there is no e-mail client loaded on the system. This was done primarily to disable an error message received every time a user logged onto the system

The Adobe Acrobat Reader was downloaded and installed from the Adobe website. This will allow users to view .pdf documents on the kiosk machine. The flash and macromedia plug-ins for Internet Explorer were also installed to provide for a better browsing environment.

Application of The NSA Template

The application of the NSA security template is a fairly simple process that has been documented a number of times. Unfortunately, at this time the administrator on each system must perform the process of applying the template using the Microsoft Management Console. For the kiosk systems, any modifications made to the template at a later date will require that an administrator manually modify each system by taking a copy of the new template file to the system and applying it. This is in part due to the severe restrictions that are to be placed on the systems to protect them from being remotely compromised. In other environments it might be possible to remotely install the security templates by using other remote management tools.

The following are the steps that were taken to perform a security analysis of the kiosk systems using the NSA Workstation security template.

- Copy or download the W2K_workstation.inf file to the kiosk system saving it in a convenient location.
- Open the Microsoft Management Console by typing “mmc” in the “run” box.
- From the taskbar select “Console” then “Add/Remove Snap-in” or use the “Ctrl-M” shortcut.
- On the “Add/Remove Snap-in” window Click “add”
- From the “Add Standalone Snap-in” window, select the “Security Configuration and Analysis” then click on “add”.
- Click “close” on the “Add Standalone Snap-in” then click “OK” on the “Add/Remove Snap-in” window

When Selecting “Security Configuration and Analysis” instructions will be provided in the main window detailing how to use the snap-in to analyze and configure the system. Figure 1. The next step will be to load the NSA template.

- Right click on “Security Configuration and Analysis” then Select “Open Database”
- As a new database is being created enter the name of the new database “NSAW2KPRO” then click “open”

- Now browse to the directory containing the "W2K_workstation.inf" file and select it.
- The NSA template is now available to be used for analyzing or configuring the system.

Next, the template will be used to analyze the system security settings,

- Right Click on the database node and select "Analyze Computer now".
- A window will open prompting for the error log file path enter a name or accept the default then click "OK".
- After the analysis is complete the system can be reviewed to determine which settings are not in compliance with the template.

Since this is a new system, there are a number of security changes to be applied. When reviewing the system template analysis, a red circle with an "x" inside shows policy mismatches. Settings that match the policy are shown with a green check mark. Figure 2.

After reviewing the changes to be made to the system, it may be necessary to modify some of the settings. As discussed earlier, the restricted groups section of the template will typically require modification as it only contains a single group. Moreover the File System section may necessitate the modification of any additional drives or folders that have been created on the system. It is important to remember that when new drives are created the default permissions will allow, "full control" to the "everyone" group! The next step is to apply the new security template to the system using the following procedure:

- Right Click on "Security Configuration and Analysis" and select "Configure Computer Now"
- A window will open prompting for the error log file path. Enter a name or accept the default then click "OK".

Testing Template Security

When preparing to test the security template, it was decided that a number of third party tools would be used. These will be followed by a number of manual tests. The combination of testing methods will guarantee the most detailed evaluation of the systems level of security. The automated tests will first insure that the installation of the system and the security template was properly executed. Next the system will be checked to determine if any connections can be made from an external system. Finally, the system will be further tested to insure it is has met the required level of security for the kiosk project. The tools to be used include the Center for Internet Security (CIS) benchmark scoring tool, Netstat, Fport and SuperScan. All of the tools used to test the kiosk system are free.

Center for Internet Security Scoring Tool

The Windows 2000 Professional Scoring tool from the Center for Internet Security[2] was used to test the system against the NSA workstation template and to determine the resulting "Score" of the system. The tool was easy to install once downloaded by following the simple Graphical User Interface. A number of

tools are included in this single package. Previously, each of these tools had to be run independently. Combining these tools makes it possible to check the system for multiple security vulnerabilities with one simple program.

Upon execution, the CIS Scoring tool will first insure that all the required security patches for both the operating system and Microsoft applications have been installed on the system. The tool will then scan the system to determine its compatibility with a selected security template. CIS provides a number of security templates including the new Windows 2000 Professional Gold Standard. The CIS scoring will then provide a "score" for the system based on the results of the system checks. A perfect score is equal to 10 points.

The CIS scoring tool has the ability to score a system based on a number of templates. As this system was configured with the NSA Windows 2000 Workstation template, that template was used for the scoring of the system as well. Following the initial run of the CIS scoring tool, the system achieved a score of "8.1". Figure 3. Unfortunately, despite the best efforts of the Microsoft "Windows Update" website, the system was still missing a hotfix which detracted greatly from the score. A missing hotfix counts for 1.25 points to be exact. After downloading and installing the Q328145 hotfix the score was increased to "9.4". Figure 4.

But why is this system not scoring a perfect 10? The score for this system was lowered by a number of Registry and file permission mismatches, 22 to be exact. In order to locate the mismatches, the Scan Log was reviewed. Then the Security Configuration and Analysis Management Snap-in was used to modify the settings as required. After a number of attempts to configure the system to conform to the standard template, there were still 4 remaining registry permissions that could not be corrected. Figure 5.

Furthermore, after manually modifying the template to the security permissions applied to the system and rescanning the system the mismatches could not be resolved. It is unclear why the system was not properly registering these values. Furthermore, it was noted that the CIS tool did not show the changes made to the permissions of the cmd.exe, tftp, ftp and telnet executables as policy mismatches. These were shown by the Security and Configuration Analysis tool and were listed as mismatches in the CIS scoring tool "Scan Log".

Netstat / Fport

Netstat is a simple command line utility included in Microsoft Windows 2000 Professional. It is used to view the status of any network connections on the local system. What is of particular interest to security practitioners is that it can display a listing of ports that are in a "Listening" status. This status means that an external computer may be able to connect to the open port allowing some type of access to the system. Allowing these connections can pose a significant security risk. In order to retrieve a list of the ports on the kiosk system, the

"netstat –an" command was used. This command provides a list of all the open ports and places them in numeric order for easier evaluation. The output of this command is show in Figure 6. A number of ports were found to be in the "listening" status. These included the TCP Ports 135, 445, 1025 and 1026 and the UDP port 445.

In the kiosk system being built for this project, the security specifications stated that there should be NO external connections made to this system. In order to prevent these connections, it is best to fully disable the processes that have placed the ports in listening status. This presents a problem in that there is no way to determine from the netstat listing what process is placing the port in the listening status. Searching Windows documentation for the information could require a significant amount of time and some of the information may never be found.

To solve this issue quickly Foundstone has developed a simple tool called Fport. This tool is available for free download from their website. With Fport it is possible to see the mapping of processes to the ports that are open. With this information now available the non-essential services can be halted. Unfortunately, some processes are required by the system and other methods of denying access to the ports must be found. The results from running fport 2.0 on the system were less helpful than had been hoped. Figure 7. None of the ports that are in listening status were mapped to processes. This will make disabling the ports more difficult as each open port will have to be researched.

After some research, it was found that Distributed Communications (DCOM) used the port 135. While most applications support DCOM it is primarily used on networked computers. As this is not a requirement of the kiosks, DCOM will be disabled. With DCOM that proved easier said than done. There are several websites with information about disabling DCOM. The most promising was http://www.uksecurityonline.com/husdg/windows2000/close135.htm. This page detailed how to disable DCOM using the dcomcnfg.exe GUI. After following the steps and rebooting the system, the port was still listening. After some supplementary research, it was discovered that the "Task Scheduler" service was responsible for the port being open. After disabling the service and rebooting the system again, the port was finally no longer in "listening" status.

Another way to disable DCOM is to change the OLE registry setting directly. This avoids the requirement to use the DCOM GUI configuration tool. This approach to the problem will also allow us to add the change to the security template before final deployment making the change automatic in all future versions of the kiosk image. HKEY_LOCAL_MACHINE\Software\Microsoft\OLE\EnableDCOM must be set to "N".

The TCP Port 445 is used by NetBIOS over TCP/IP. Since the kiosk systems are not using networking resources, NetBIOS can be disabled. Disabling it was quite well documented on the website located at http://www.uksecurityonline.com/husdg/windows2000/close445.htm. The process consisted of editing the registry setting HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/Services/NetBT/Parameters/TransportBindName. The default setting of \Device\ must be removed and the Value Data left blank. Figure 8

The final netstat performed on the system showed that no ports were in a listening status Figure 9. At this point, the system is virtually invisible to the surrounding network and has no capability of negotiating incoming connections. For confirmation that no ports were listening, the system was tested using the SuperScan tool available from Foundstone[3]. This tool confirmed that the system did not respond to any external requests.

Local Access Security Tests

Several local tests were performed to insure that the security template was properly protecting the system. A test was performed to insure that the system was properly auditing events. The administrator account was used to attempt to create a new user account on the system. The Event log was then checked to confirm that the "use of privilege" was logged. As was expected, the log reflected the account management activity shown in Figure 10. By logging the use of privileges, it is possible to track changes to the system which could create serious changes to the security profile of the system.

In order to test how the security template protects the system from local users, a number of attempts were made to perform actions that should not be allowed by a user of the kiosk system.

To check the "user rights assignments" modifications made to the system, an attempt was made to edit the security event log using the "kiosk" user account. The NSA template configured the system to restrict all attempts to access the security logs to the administrator account and the user was denied as expected. By restricting access to the security logs, a user is prevented from deleting any auditing information gathered by the system on their actions. This will prevent a hacker from "covering their tracks" This is shown in Figure 11.

To check file permissions configured by the template, an attempt was made to save a file downloaded from the Internet. The first check preformed was to try and save the file to the System Drive C:/ and several sub-folders. All attempts were denied except for those made to the Documents and Settings/kiosk users folder. The "kiosk" user by default has "full control" of it's own directory.

The template performed excellently on the remainder of the system drive as it limited all other access to the read/execute/list folder contents permissions.

However, the d:\ drive added during the installation was not configured by the template and currently has permissions allowing the "everyone" group full control. The final deployment template will be modified to restrict the "kiosk users" group, as this drive should have its permissions checked in order to protect it from local users!

Although not directly related to the template applied, there were a number of other security issues that were tested. An attempt was made to add a file to the startup folder. This action could allow a user to force an executable to initialize at the user level of the next person to login to the system. In the case that the executable was placed in the administrator's startup folder, the results to the system could be catastrophic. Fortunately, the test failed when trying to add the file to the "administrator", "default user" and "all user" startup folders!! It was however possible to add the file to the "kiosk" user account. This could still allow a user to install a keystroke logging utility to the system and configure it to automatically start each time the "kiosk" user logs in allowing the user to gather user accounts and passwords of other users. The permissions on the startup folder for the kiosk account will be modified to prevent files from being added by the "kiosk user" group.

Testing Template Functionality

Testing was performed to insure that the functionality of the kiosk system was as specified in the requirements. As this system had few requirements, it was doubtful that the system would not meet the functionality requirements. More concern was placed on restricting the functionality to the minimum level. In order to test the system, a simple checklist was created based upon the initial requirements gathered during the planning phase.

All of the system testing was performed using the "kiosk" user account. The obvious first test was to insure that the system could be connected to a network and acquire an IP address using DHCP. There was some concern that this feature would work properly after disabling the DCOM features during the hardening of the system. It appears that in the environment used the system was capable of requesting an IP address.

The next step was to confirm that the "kiosk" user could execute the Internet Explorer browser application and connect to the Internet. This was performed by connecting to a number of websites with varying content types to insure that sites were viewed correctly. While testing these sites, a number of documents were requested that use the Adobe Acrobat™ format (.pdf). Sites were also tested that included Flash™ and other enhancements.

Testing was also performed to insure that the web browser could successfully connect to secure websites and authenticate. This is a requirement for using web based e-mail and web portal applications that are essential to the kiosk projects success. A number of public e-mail sites including Yahoo™ and

Hotmail™ were tested for compatibility. A final test was performed using the corporate web portal to access a number of systems located on the internal network including the e-mail web client. All of these tests were easily passed by the system.

During this testing a number of concerning observations were made by the testers. The system allows the kiosk user to execute a number of applications that are not necessary for a system designed only to allow web access. Several of the most dangerous programs were disabled during the hardening phase. The testing group has commented that perhaps the system should be further stripped down in order to remove all the applications from the desktop and start menus except the Internet Explorer browser.

Testers were very concerned that the system desktop background and many other settings could be changed by the kiosk user and were permanently saved. They also noticed that despite the fact that Internet Explorer browser was configured not to save history information the kiosk user could modify the Internet options to enable the feature. The browser default homepage and other settings could also be manipulated.

A security template would not be capable of preventing these changes. Many of the executable files can be removed from the start menu to solve the execution problems. Ultimately, to fully solve the issues with the system and IE settings and to restrict the use of local applications a Local Computer group policy will be required.

Evaluation of the Template

The NSA template provides for a number of configuration changes with a minimum of time and effort. The template efficiently removed many security vulnerabilities common to a workstation in a corporate environment. As stated repeatedly in the documentation provided by the NSA, several sections of the template require some customization before it can be used. This is to provide the necessary variables based on the environment where the template is to be used.

For this application, it was necessary not only to customize the required sections of the template but also to change a number of the individual settings. Several settings were not optimal for a kiosk environment. This is primarily because a single user account is shared by a number of users and has a blank password. Due to this access provided to the user must be very tightly controlled.

In the Account Policies Section changes were made to eliminate the password history, maximum password age and minimum password length. As the only user account with a password is the Administrator account these settings would only be an annoyance following deployment.

Changes were made to the “User Rights Assignment” section of “Local Policies” in order to reduce the rights of normal users. The “access this computer from the network” and “ Shut down the system” rights were removed from “users”. This will prevent anyone other than administrators from accessing or rebooting the system. Allowing the compute to be rebooted could provide the potential for a local user to perform changes to the system boot process by inserting a boot disk at startup. As all the ports are closed on the system and the hardware locked out of reach these changes are based primarily on paranoia.

In the “Security Options” section it was necessary to provide the template with the new administrator and guest account names. Additional security options were added to the system by editing the sceregvl.ing file as described in Appendix A. The updates made to this file will have to be manually applied to each system. These changes allow the template to Disable Distributed Communications (DCOM) and NetBIOS over TCP/IP as was performed during the testing phase of the initial system.

The “kiosk user” group was added to the restricted groups and the “kiosk” account added as a member of the group. This will insure that the restrictions applied to the “kiosk user” group will properly apply to the “kiosk” account.

As determined during testing, the “Task Scheduler” service had to be disabled in order to close port 135 on the system. To simplify this process in the future, the process was disable in the template. The NSA template did not define any of the system services assuming that they would be at the default settings. To confirm the service status and protect the system, it was decided to set all the unused services to “Disabled” to prevent their unauthorized use. Particular attention was paid to insure that all services providing for remote access to the system were disabled. These include; remote registry service, remote access connection manager, telnet and network DDE. The Event Log service was also forced to “automatic” to insure that it is has not been disabled. Finally, the “kiosk user” group was restricted from making any changes to the status of services on the system.

Several modifications were made to the File system section of the template. Several files including ftp.exe, tftp.exe, command.com, mmc.exe and cmd.exe were modified to prevent the “kiosk user” group from executing them. The entire “kiosk” users “documents and settings” folder was set to deny write permissions to the “kiosk user” group preventing any changes from being made. The “d:\” drive settings were modified to remove the “Everyone” group permissions and the Administrator was given full control. These settings were in response to several security issues noted during system testing.

Conclusion

The NSA template provided for a number of configuration changes to increase the security of the system and saved a vast amount of time in implementing

them. A considerable amount of time and energy was spent during this project to customize and improve the NSA template for this application. Even with the modified template available for building the future systems there will still be a great deal of work required to secure the systems. The entire procedure for this project was repeated in order to confirm the procedure. The process required almost 4 hours to complete including the base installation, patching, hardening and template application. That is a considerable amount of time to build a secure system with so few applications. It would be difficult to estimate how many additional hours would be required were it not for the security templates.

A this point in order to enforce many of the additional restrictions of the security requirements it will be necessary to create a group policy to be applied to the system. This will increase the difficulty of building multiple systems given that Microsoft has no way of exporting and importing the local computer group policies. There are some third party products such as FAZAM that will make the process easier and will be reviewed to determine what benefits they may provide to the completion of this project.

Images…

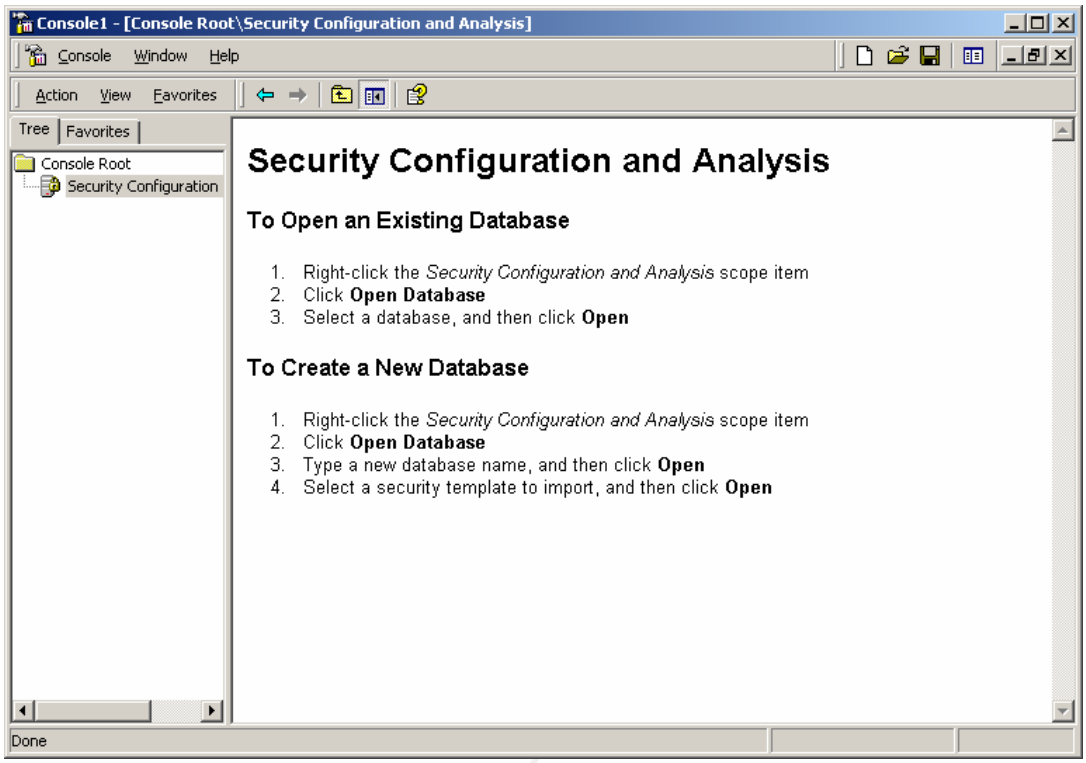

Figure 1

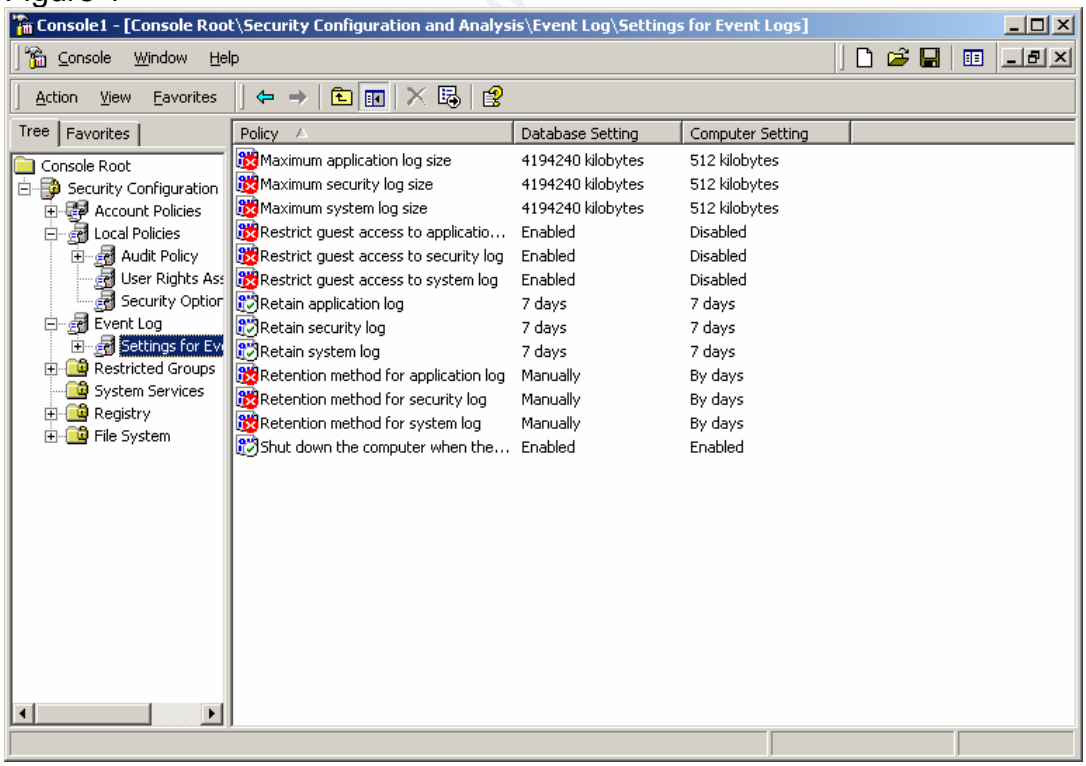

Figure 2

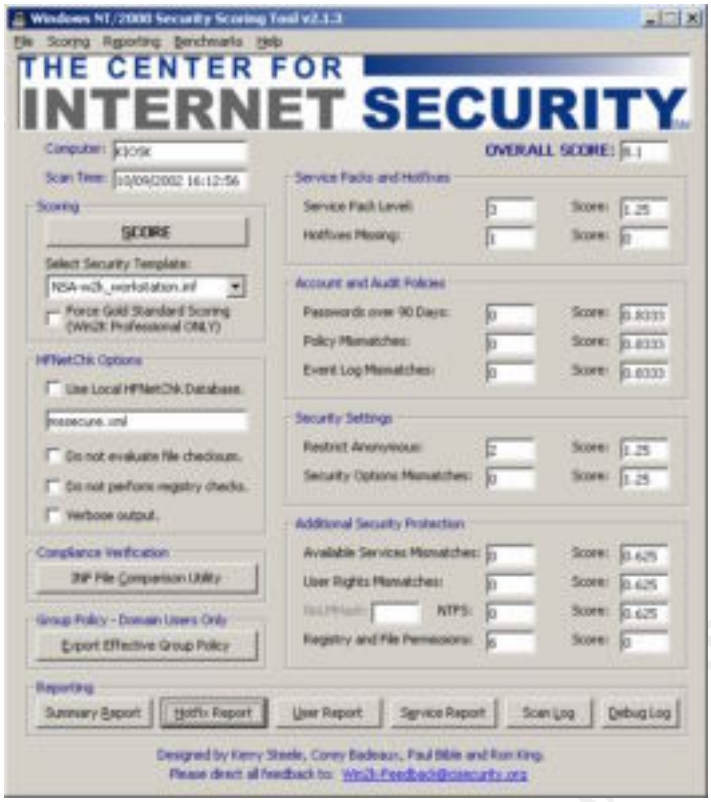

Figure 3

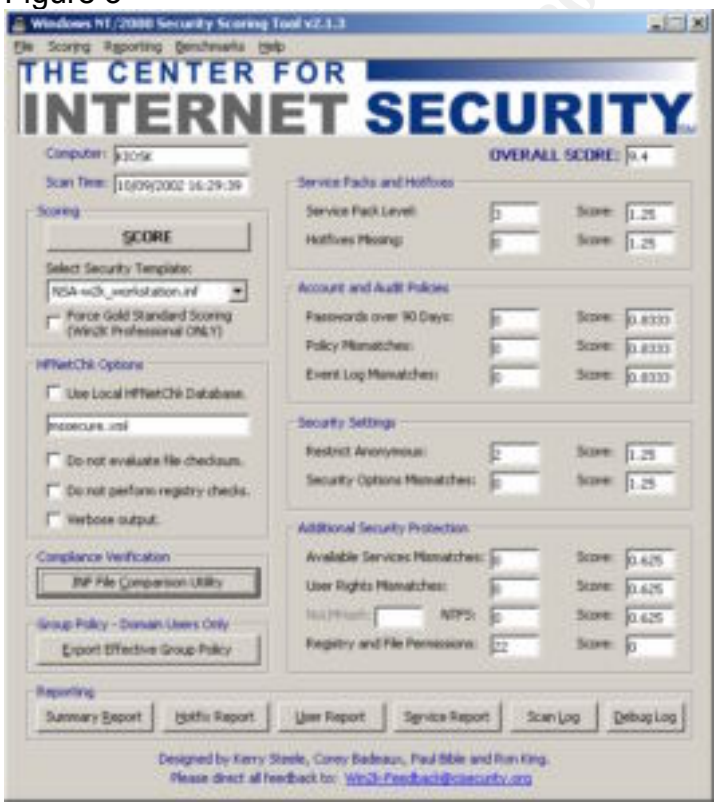

Figure 4

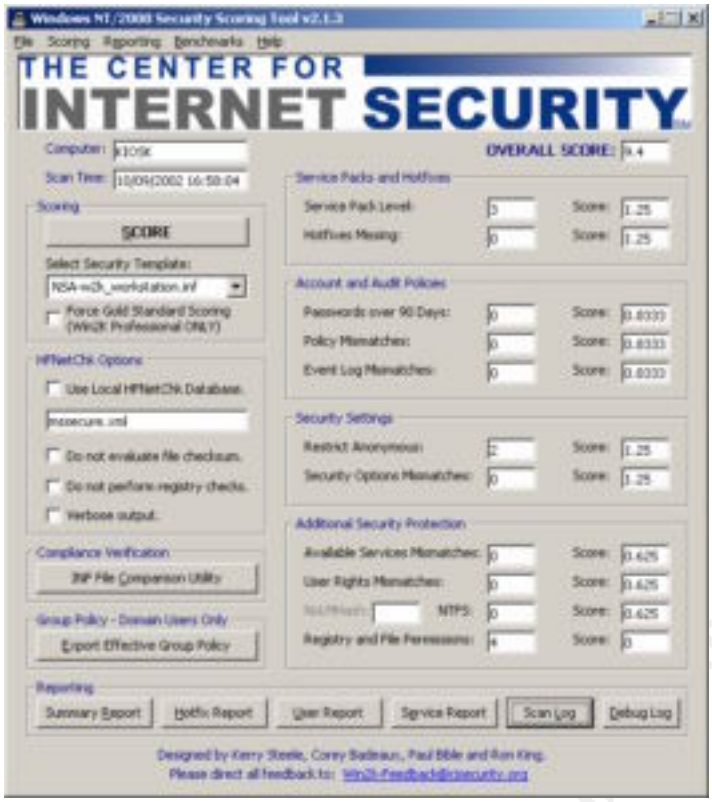

Figure 5

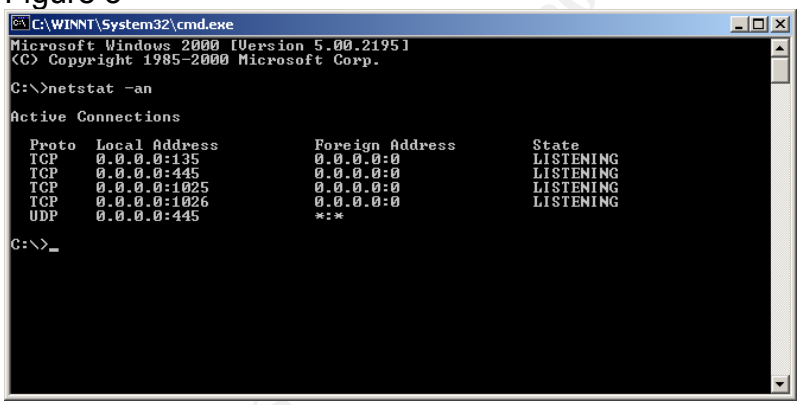

Figure 6

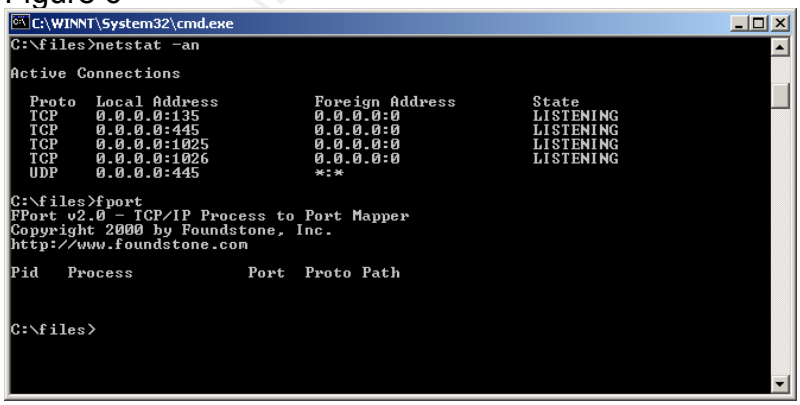

Figure 7

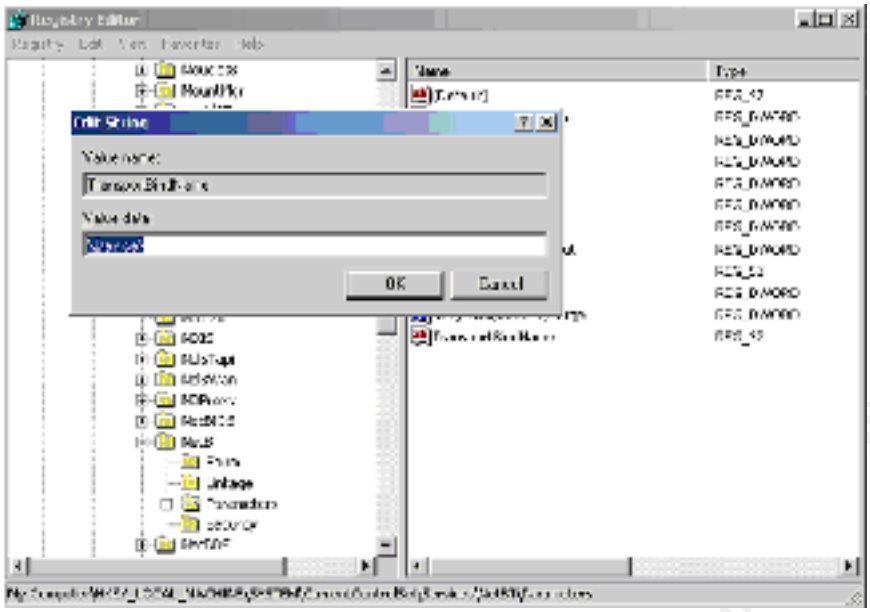

Figure 8

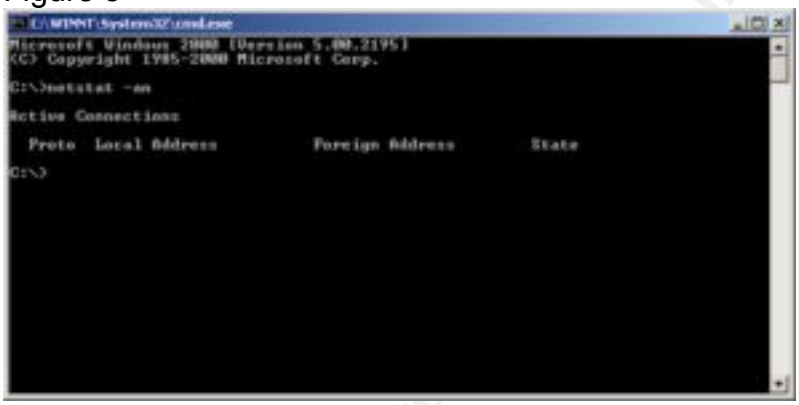

Figure 9

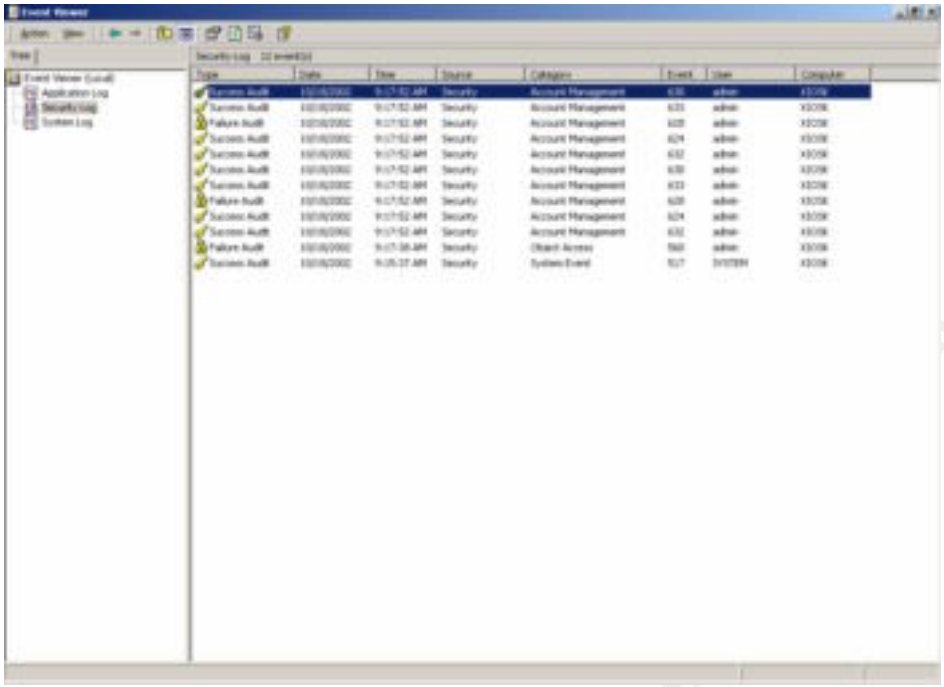

Figure 10

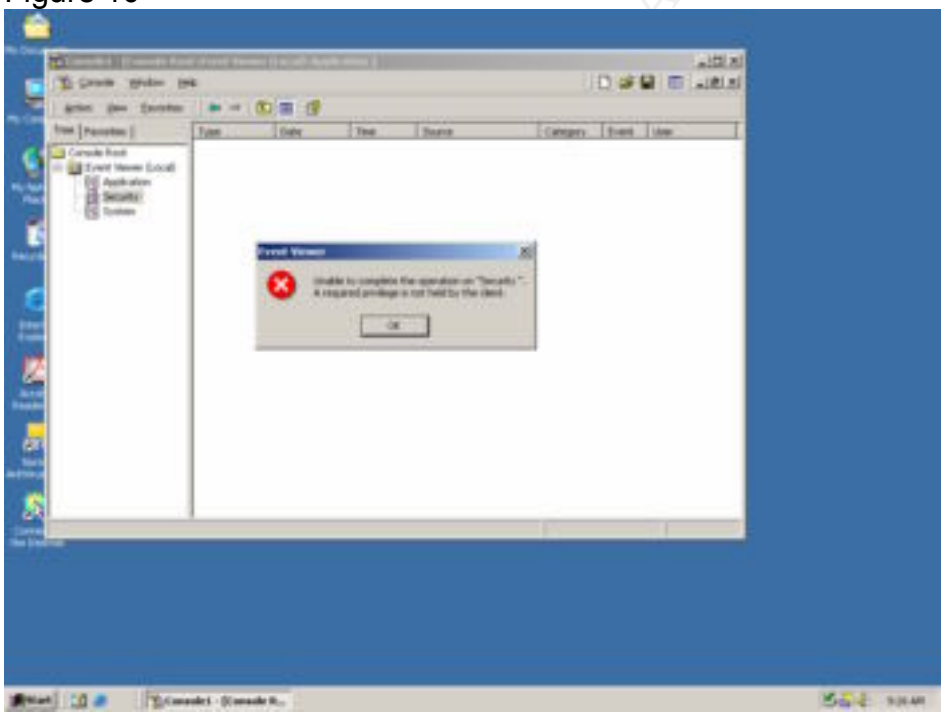

Figure 11

Appendix A

"In the Windows 2000 Security Configuration Tool Set, it is possible to add additional registry key settings to the Security Options portion of a template. To accomplish this, perform the following actions:

- _ Open the file %SystemRoot%\inf\sceregvl.inf (%SystemRoot% is usually C:\winnt) in Notepad, Wordpad, or another text editor
- _ Add a line in the form *regpath, type, displayname, displaytype* where
  - _ *regpath* – registry key value path, e.g.,
  - MACHINE\System\CurrentControlSet\Control\Lsa\AuditBaseObjects
- _ *type* – data type of the registry entry represented by a number. Possible values are REG_SZ (1), REG_EXPAND_SZ (2), REG_BINARY (3), REG_DWORD (4), REG_MULTISZ (7)
- _ *displayname* – the name actually displayed in the security template, e.g., "Audit the access of global system objects"
- _ *displaytype* – How the interface will display the registry value type. Possible
- values are Boolean (0), number (1), string (2), choices (3). If choices are specified, the choices should then be specified in the format *value1|display1,value2|display2,…*
- _ Re-register scecli.dll by executing regsvr32 scecli.dll at a command prompt

An example line in sceregvl.inf is:

MACHINE\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon\ScRemoveOption,1
,%ScRemove%,3,0|%ScRemove0%,1|%ScRemove1%,2|%ScRemove2%

The strings listed above are defined in the [Strings] section of sceregvl.inf:
%ScRemove% = Smart card removal behavior
%ScRemove0% = No Action
%ScRemove1% = Lock Workstation
%ScRemove2% = Force Logoff"[4]

Authors Note…

At the time that this project was begun, the Windows 2000 Professional "Gold Standard" template was not yet released. As such a great amount of work had already been done by the time it was the decision was made not to change base templates. Had this project begun today it would be the most obvious choice of templates. Ultimately given the abnormal requirements of a kiosk system the template would still require a great amount of customization.

Additional References:
http://www.hsc.fr/ressources/breves/min_srv_res_win.en.html
http://www.usenix.org/publications/login/2000-2/features/bastionhost.html

---

[1] *Guide to Securing Microsoft Windows 2000 Group Policy: Security Configuration Tool Set,* http://nsa1.www.conxion.com/win2k/guides/w2k-3.pdf
[2] http://www.cisecurity.org/bench_win2000.html
[3] http://www.foundstone.com/knowledge/proddesc/superscan.html
[4] *Guide to Securing Microsoft Windows 2000 Group Policy: Security Configuration Tool Set,* http://nsa1.www.conxion.com/win2k/guides/w2k-3.pdf