GIAC Certified Windows Security Administrator (GCWN) Practical Assignment Version 3.1 (revised April 8, 2002)

Option 2 – Securing Windows 2000 With Security Templates

SANS/NISER Asia Pacific Conference
Kuala Lumpur, Malaysia
October 7-12, 2002

Prepared by Gerald Chuah

March 10th, 2003

Table of Contents

1. Introduction 3
   1.1 Executive Summary 3
   1.2 Environment 3
   1.3 Assumptions 3
2. Description of System 5
   2.1. Type and Role of System 5
   2.2. Hardware and Software Specification 5
   2.3. System's Security Requirements 11
3. Template Selection 12
   3.1. Selecting a Template 12
4. Security Settings 13
5. Apply, Test, and Evaluate the Template 26
   5.1. Apply The Template 26
   5.2. Test The Template's Security Settings 31
   5.3. Test the System's Functionality 36
   5.4. Evaluate the Template 41
6. Conclusion 44
7. References 45
8. Appendix A w2k_workstation.inf Template 46

1. Introduction

1.1 Executive Summary

It takes considerable time and effort to select the right security template for the right environment. This is more evident with numerous checklist and documents that have been developed to secure Windows 2000. (The SANS Institute, Microsoft, The NSA, The Center for Internet Security etc)

The paper explains how to apply, test and evaluate a security template on a Windows 2000 professional business workstation. The document will address a project by CRSB to implement a business workstation. The template that is discussed is Windows 2000 Workstation template by the National Security Administration of the United States of America.

1.2 Environment

CRSB is a retail outlet providing computer sales and services. There are two Microsoft Windows NT 4.0 servers and 8 Windows 98 workstations. The Management has decided to install a business workstation that functions like a kiosk to provide internet services for its customers.

The workstation will allow customers and employees to access the internet. Customers will be able to check e-mail using internet mail service like Hotmail or Yahoo.They will be able to browse websites using either secure (https) or insecure (http) sites.They are able to use WordPad to create documents.

These workstations will be placed in all CRSB retail outlets. This simple requirement creates security issues that needs to be considered. The system must be protected from being compromised both from customers and employees. This will be discussed later in the security requirement.

1.3 Assumptions

The following essential assumptions have been made to limit the scope of this document:

- The business workstation is not connected to Local Area Network. There will be separate network connectivity and firewall protection.
- The business workstation are Intel-based architecture and will be cleanly installed with Microsoft Windows 2000 Professional, not upgraded.
- The latest Windows 2000 service pack and hotfixes will be installed. For

further information on critical Windows 2000 updates, refer to Windows Update for Windows 2000 web page http://windowsupdate.microsoft.com or search for security hotfixes by service pack at the Technet Security Bulletin Search http://www.microsoft.com/technet/security/current.asp.

- Applications are Windows 2000 compatible. The applications used will be Internet Explorer and WordPad.

2. Description of System

2.1. Type and Role of System

The type of system to be secured is a Windows 2000 Professional business workstation. The workstation's role is similar to a kiosk where it will be used for the Web mail and Web browsing. This includes using WordPad to create documents. The workstation will only allow access for any user to secure (https) or unsecure (http) websites. It will also allow any user to check e-mail using Internet mail services like Yahoo mail or Hotmail. It will enable users to create documents with WordPad.

2.2. Hardware and Software Specification

The system is based on the standard Personal PC platform.

Hardware Configuration

Digitech OEM Personal Computer

Processor:	Pentium III
Memory:	256 MB RAM Memory
Hard disk:	10GB
Video:	8MB
CD-ROM:	50x
Network Card:	Any Ehthernet Adapter

Software Installed

As this system will be used as a workstation, Microsoft Windows 2000 Professional SP3 with Internet Explorer as the web browser was chosen. This is due to a number of reasons. This product is familiar to everyone and is user friendly. The web browser Internet Explorer is most widely used and compatible with most web sites and portal.

McAfee VirusScan 4.5.1 SP1 will be used as the virus scanning software. It will be configured to protect against malware that may be downloaded from internet or embedded scripts using java or ActiveX from certain web sites. It will be configured to receive Virus definition updates as they become available.
The configuration details is outside the scope of this paper.

No other software will be installed. Some applications like WordPad is part of the default installation. Most application included with Windows 2000 Professional will not be installed during the initial build of the system. Reducing the number of software will reduce risks of security vulnerabilities.

Windows 2000 Professional Installation

Windows 2000 Professional was installed from the Windows 2000 Professional CDROM without any connection to the network. All drives were formatted with NTFS to support Access Control Lists (ACL).

The system was installed at the default location, which is C:\WINNT.

Post Windows 2000 Professional Installation

The latest service pack which is SP3 was installed to ensure the workstation is up to the latest security level. This includes installing any security hot fixes and patches.

SP3 was obtained from
http://www.microsoft.com/windows2000/downloads/servicepacks/default.asp

After SP3 was installed the workstation was rebooted.

Hotfixes and Patches

One of the more popular tools to determine which hotfixes are needed is Hfnetchk. Hfnetchk is a command line tool to check a computer or a group of computers to determine whether a specific patch is installed by by evaluating and verifying three items:

The registry key that is installed by the patch
The file version
The checksum for each file that is installed by the patch.

Hfnetchk can be downloaded from:

http://hfnetchk.shavlik.com/default.asp

The Hfnetchk tool was run from the command line to check the patch status against the mssecure.xml database downloaded on 20th January 2003. The following syntax was used to generate the patch report below:

hfnetchk -v -s 1 –x mssecure.xml

The switches tell Hfnetchk to do the scan with the following changes:

Output verbose or detailed mode (-v)
Do not display note messages (notes are messages and can not be fixed by just the installation of a patch) (-s 1)
Specify the XML datasource containing the hotfix information (-x mssecure.xml)

DIGITECH (192.168.247.128)
---

* WINDOWS 2000 SP3

Patch NOT Installed MS02-042 Q326886
File C:\WINNT\system32\netman.dll has a file version [5.0.2195.5282] that is less than what is expected [5.0.2195.5974].

Patch NOT Installed MS02-045 Q326830
File C:\WINNT\system32\xactsrv.dll has a file version [5.0.2134.1] that is less than what is expected [5.0.2195.5971].

Patch NOT Installed MS02-048 Q323172
File C:\WINNT\system32\xenroll.dll has a file version [5.131.2510.0] that is less than what is expected [5.131.3659.0].

Patch NOT Installed MS02-050 Q329115
File C:\WINNT\system32\adsldp.dll has a file version [5.0.2195.5400] that is less than what is expected [5.0.2195.5781].

Patch NOT Installed MS02-055 Q323255
File C:\WINNT\hh.exe has a file version [4.74.8793.0] that is less than what is expected [5.2.3644.0].

Patch NOT Installed MS02-063 Q329834
File C:\WINNT\system32\drivers\raspptp.sys has a file version [5.0.2195.4080] that is less than what is expected [5.0.2195.6076].

Patch NOT Installed MS02-069 Q810030
File C:\WINNT\system32\msjava.dll has a file version [5.0.3805.0] that is less than what is expected [5.0.3809.0].

Patch NOT Installed MS02-070 Q329170
File C:\WINNT\system32\spoolss.dll has a file version [5.0.2195.5400] that is less than what is expected [5.0.2195.6047].

Patch NOT Installed MS02-071 Q328310
File C:\WINNT\system32\basesrv.dll has an invalid checksum and its file version [5.0.2195.5265] is equal to what is expected [5.0.2195.5265].

* INTERNET EXPLORER 5.01 SP3

Patch NOT Installed MS02-009 Q318089
File C:\WINNT\system32\vbscript.dll has an invalid checksum and its file version [5.1.0.7426] is equal to what is expected [5.1.0.7426].

Patch NOT Installed MS02-066 Q328970
File C:\WINNT\system32\mshtml.dll has a file version [5.0.3502.5390] that is less than what is expected [5.0.3510.1100].

* WINDOWS MEDIA PLAYER 6.4 GOLD

Patch NOT Installed MS02-032 Q320920
File C:\WINNT\system32\msdxm.ocx has a file version [6.4.9.1121] that is less than what is expected [6.4.9.1124].

* MDAC 2.5 SP3

Patch NOT Installed MS02-065 Q329414
File C:\Program Files\Common Files\System\msadc\msadce.dll has a file version [2.53.6200.0] that is less than what is expected [2.53.6202.0].

```
Select C:\WINNT\System32\cmd.exe

C:\Program Files\Shavlik Technologies\HFNetChk>Hfnetchk -v -s 1 -x mssecure.xml
Shavlik Technologies Network Security Hotfix Checker 3.86
Copyright (C) 2001-2002 Shavlik Technologies, LLC
Shavlik Technologies, LLC
info@shavlik.com (www.shavlik.com), 651-426-6624
All Rights Reserved


Attempting to load mssecure.xml.

================================================================

Scan performed Fri Jan 24 21:03:39 2003
Shavlik Technologies Network Security Hotfix Checker, 3.86
Using XML data version = 1.1.1.573  Last modified on 1/20/2003.



Scanning DIGITECH
..................
Done scanning DIGITECH
------------------------------
DIGITECH (192.168.247.128)
------------------------------

        * WINDOWS 2000 SP3

        Patch NOT Installed      MS02-042        Q326886
        File C:\WINNT\system32\netman.dll has a file version [5.0.2195.5282]
        that is less than what is expected [5.0.2195.5974].


        Patch NOT Installed      MS02-045        Q326830
        File C:\WINNT\system32\xactsrv.dll has a file version [5.0.2134.1]
        that is less than what is expected [5.0.2195.5971].


        Patch NOT Installed      MS02-048        Q323172
        File C:\WINNT\system32\xenroll.dll has a file version [5.131.2510.0]
        that is less than what is expected [5.131.3659.0].
```

Hfnetchk Scan

All outstanding hotfixes were installed and the machine rebooted for the updates to take effect. Following a reboot of the machine, the Hfnetchk scan was run with the following :

hfnetchk -v -s 1 –x mssecure.xml

DIGITECH (192.168.247.128)
---

* WINDOWS 2000 SP3

Information
All necessary hotfixes have been applied.

* INTERNET EXPLORER 5.01 SP3

Information
All necessary hotfixes have been applied.

* WINDOWS MEDIA PLAYER 6.4 GOLD

Information
All necessary hotfixes have been applied.

* MDAC 2.5 SP3

Information
All necessary hotfixes have been applied.

Mcafee Antivirus virus definitions were updated and AutoUpdate was configured to update once a week to the Mcafee ftp server. A scan for viruses was done on the machine.

System Hardening

At this stage the Operating system installation is complete and all necessary Hotifx and patches have been installed. Several steps needs to be done to harden the system.

The administrator account is renamed and default description is changed to protect the account. The guest account is also renamed and default description changed and the account is left disabled.

A new account called Administrator is created and disabled. This account is a regular user account belonging to the user group. This account will act like a "bait" that hackers can try to hack. This is done as a precaution to warn the real administrator that someone is trying to access the system.

A kiosk account with no password is created. This account will allow access for kiosk users.

The default networking settings is modified to remove all unnecessary bindings. File and Print Sharing for Microsoft Networks and Client for Microsoft Networks bindings are removed from the system. This will prevent users from creating local shares or map drives to shares on other systems. Support for NetBios is also disabled, this is done by changing TCP/IP properties "Advanced" section "Wins" configuration tab.

Finally to prevent it from being used to attack remote systems or locally exploited, NTFS permissions for telnet, FTP, TFTP, mmc(Microsoft Management Console) and cmd executables is changed.

2.3. System's Security Requirements

To determine the security requirement, it is important to identify the risks

involved. One method would be to access the system's potential weakness.

The business workstation will be accessible to everyone. The system must be protected against theft. Therefore steps have been taken to lock the CPU, keyboard and mouse. This is done by mounting it on a special table in the showroom area of all retail outlets. This will prevent access to floppy drives and CDROM. This helps to avoid installation of malware, Trojan programs that can bypass NTFS file system and access the hard disk files. This will prevent installation of hardware keystroke devices that can steal usernames and passwords. All staf on duty at the showroom area are reqested to keep a close eye on any suspicious activity that customers may be doing while using the system

As users from outside the company will use this system, it will not be connected to the company's local area Network. Additional telecommunication facilities will be required to connect the workstation to the Internet. These facilities can consist of cable modem connection or DSL.

The system will need protection from external access. A firewall solution is needed but is outside the scope of this paper. A virus scanning software discussed in the previous section will be installed to protect against virus and malware programs.

Users will be able to access the workstation with a pre-defined user account. The account used will not require a password and can use a blank password. There would be limited amount of protection provided with a user account, therefore the level of access that is provided must be tightly controlled. User must not be allowed to run any application except Internet Explorer browser and WordPad. User cannot be allowed to change any system settings, install software, save files from the internet except to its own user directory, resart system, start or stop services, view or change any of the log files, delete system or application files. FTP, TFTP and telnet services will be disabled to reduce the risk of unauthorised access to other systems.

Internet Explorer will be configured not to store any information from sites visited in cache files, the Internet history log of previously visited sites will be disabled and disable storage of cookie files to prevent storage of users credentials.

3. Template Selection

3.1. Selecting a Template

An existing template, provided from a reputable source (e.g. Microsoft, the National Security Agency (NSA), SANS, etc.) ensures a reliable security baseline in hardening the operating system. Since this business workstation functions as a kiosk, the workstation template would be most appropriate. There are a few templates for the workstation like NSA, Microsoft etc.

The template selected would need to satisfy the security requirements described earlier and should be as restrictive as possible. Therefore the National security Agency Windows 2000 workstation template was chosen. NSA is a highly respected source for security baselines, they have provided advice on configuration for Unix, Microsoft, Cisco for a number of years. The settings in this template are based on Microsoft hisecws.inf template. It provides enhanced security settings and is extremely well documented. The NSA provides a well-documented description of its templates that can be downloaded from: http://nsa2.www.conxion.com/win2k/download.htm.

4. Security Settings

Before deployment of NSA w2k_workstation.inf template a review of its security settings will be conducted. The template makes several changes to the Account Policies, Local Policies, Event Log, Restricted Groups, System Services, Registry and File System security settings. All relevant security settings to the business workstation are explained in this section. For more detailed information on other settings modified by the template refer to NSA Guide to Securing Microsoft Windows 2000 Group Policy: Security Configuration Tool Set.

Account Policies

This section includes Password Policy, Account Lockout Policy and Kerberos Policy. Since Active Directory is necessary for Kerberos authentication and Active Directory is not deployed, Kerberos policies are not required.

Password Policy

Enforce password history - 24 passwords remembered

Prevents users from reusing their previous 24 passwords. Reduce risk of hackers discovering passwords

Maximum password age - 90 days

The period of time the password is valid before it has to change

Minimum password age - 1 day

The period of time the password is valid before it can be changed

Minimum password length - 12 characters

The least number of characters for an account's password. The longer it is the more difficult it is to crack. This will reduce the chances of a password being cracked by password cracking tools.

Password must meet complexity requirements – Enabled

This option determines whether passwords must meet the following complexity requirements.

- Does not contain all or part of the user's account name
- Must be least six characters in length
- Contains characters from three of the following four categories:

- Upper case characters (A-Z)
- Lower case characters (a-z)
- Numbers (0-9)
- Symbols (!$#% etc..)

With password complexity enabled, the ability to thwart malicious users in trying to guess the password is greatly increased.

Store password using reversible encryption for all users in the domain - Disabled

Storing passwords with this method is the same as storing the password in clear text and should NEVER be enabled.

Account Lockout Policy

Account lockout duration - 15 minutes

Determines the number of minutes that a user account is locked out.

Account lockout threshold - 3 invalid logon attempts

Limits the amount on invalid logon attempts to 3 before the account is locked out.

Reset account lockout counter after - 15 minutes

The number of minutes before a locked out account's failed logon attempts are reduced to 0.

Changes to the password policy provide stronger passwords, making passwords harder to guess, steal and extract with a password cracking utility. Changes to the account lockout policy are intended to lock accounts when an invalid password is entered three times. There is a 15 minutes delay before the account is unlocked. This prevents malicious users from guessing the passwords by brute force, known as a dictionary attack. A dictionary attack is an attack that tries to potentially send thousands of account password attempts relying on a predefined list of passwords.

Local Policies

This section includes audit policy, user righs assignment and security options.

Audit Policy

Audit account logon events - Success, Failure

Records when an attempt to logon to an account is successful or fails.

Audit account management - Success, Failure

Records events that are related to account management. Specifically when user accounts are changed, added, and deleted. Also, any password changes are captured as well.

Audit directory service access – No auditing

Applies to Active Directory so this is not applicable.

Audit logon events - Success, Failure

Records each occurrence of an account logging on, logging off, or making a network connection to this server.

Audit object access - Failure

Records failed access to objects such as files, directories, registry keys and printers.

Audit policy change - Success, Failure

Records successful and failed changes to the user rights policies and audit policies.

Audit privilege use - Failure

Records attempts to exercise a right that has not been assigned to the particular user.

Audit process tracking - No auditing

If activated, this would facilitate the generation of an event that details program activation and exits. With the setting activated, a substantial additional amount of logging activity may be generated. This could also affect both performance and disk storage. This setting is useful for short-term activation when the need arises.

Audit system events - Success, Failure

Records when account initiates a shutdown or restart of the server. Also, any events that affect the server security are recorded here.

Auditing collects information about system usage. It is a method of maintaining

logs of information that describes in details events that have taken place on the system. Since Windows 2000 Professional disables all auditing by default , it is necessary to enable auditing. Auditing will help to monitor for any suspicious activity that may indicate the system was compromised.

User Rights Assignment

Access this computer from the network - Administrators, Users

Allows Administrators and Users to connect over the network.

Act as part of the operating system - Not defined

Not applicable

Add workstations to domains - Not defined

Not applicable

Backup files and directories - Administrators

Allows only Administrators the privilege of bypassing file and directory permissions in order to backup the system. This is an override to the regular file and directory permissions.

Bypass traverse checking – Users

Allows Users to bypass the normal restrictive permissions on a directory and permits them to ability traverse the directory trees.

Change the system time - Administrators

Allows Administrators to change the date and time on the system

Create a pagefile - Administrators

Allows only Administrators the privilege to create and modify the size of a pagefile (i.e. known as Virtual Memory).

Create a token object - Not defined

Not applicable

Create permanent shared objects - Not defined

Not applicable

Debug programs - Not defined

Not applicable

Deny access to this computer from the network - Not defined

Not applicable

Deny login as a batch job - Not defined

Not applicable

Deny logon as a service - Not defined

Not applicable

Deny logon locally - Not defined

Not applicable

Enable computer and user accounts to be trusted for delegation - Not defined

Not applicable

Force shutdown from a remote system - Administrators

Allows Administrators the privilege to shutdown the system remotely.

Generate security audits - Not defined

Not applicable

Increase quotas - Administrators

Not applicable

Increase schedule priority - Administrators

Not applicable

Load and unload device drivers - Administrators

Not applicable

Lock pages in memory - Not defined

Not applicable

Log on as a batch job - Not defined

Not applicable

Log on as a service - Not defined

Not applicable

Log on locally – Administrators, Users

Allows Administrators and Users the privilege to logon at a system console.

Manage auditing and security log - Administrators

Not applicable

Modify firmware environment values – Administrators

Not applicable

Profile single process – Administrators

Not applicable

Profile system performance – Administrators

Not applicable

Remove computer from docking station – Administrators, Users

Not applicable

Replace a process level token - Not defined

Not applicable

Restore files and directories – Administrators

Allows Administrators to bypass file and directory permissions when restoring

files and directories that have been backed up.

Shut down system – Administrators, Users

Allows Administrators and Users to shut down Windows 2000.

Synchronize directory service data - Not defined

Not applicable

Take ownership of files or other objects - Administrators

Allows administrators to take ownership of files, directories, printers and other objects.

User rights policy limits specific actions to specific users. This prevents users from tasks that should be reserved for administrators. Some examples include Shut down system, take ownership of files or other objects, Log on locally.

Security Options

Additional restrictions for anonymous connections - No access without explicit anonymous permissions

Any anonymous connections must be granted explicit privileges to any required resources. Specifically, Everyone and Network are removed from the anonymous users token.

Allow Automatic Administrator Logon – Disabled

Allows a system to automatically logon as administrator when mahine is started This is disabled by default

Allow server operators to schedule tasks (domain controllers only) - Not defined

Not applicable

Allow system to be shut down without having to logon - Disabled

Users must be ale to logon to the system to shutdown the computer

Allow to eject removable NTFS media - Administrators

Only Administrators are allowed to eject removable NTFS media

Amount of idle time required before disconnecting session - 30 minutes

Specifies that 30 minutes of continuous idle time must pass in a Server Message Block session before the session is terminated due to inactivity.

Audit the access of global system objects – Enabled

Enables objects such as semaphores, mutexes, etc., to be created with System Access Control Lists (SACLs) that can then be used to audit any access to these objects.

Audit use of Backup and Restore privilege - Enabled

Enables auditing of user rights including Backup and Restore which can be recorded in the security log if "Audit privilege use" is enabled as well.

Automatically log off users when logon time expires - Not defined

Not applicable

Automatically log off users when logon time expires (local) - Enabled

Disconnects any SMB client sessions to be disconnected when client's logon time expires.

Clear virtual memory pagefile when system shuts down – Enabled

The Virtual Memory pagefile is cleared after a clean shutdown.

Digitally sign client communication (always) – Disabled

Not applicable

Digitally sign client communication (when possible) - Enabled

An SMB client connection is required to perform SMB packet signing when communicating with an SMB server that also support packet signing.

Digitally sign server communication (always) - Disabled

Not applicable

Digitally sign server communication (when possible) - Enabled

Enables the SMB server to perform packet signing.

Disable CTRL+ALT+DEL requirement for logon - Disabled

Requires CTRL+ALT+DEL before logon. Not disabling this before the logon may leave the connection open to a malicious user to intercept the password.

Disable Media Autoplay - All Drives

Disable all media from executing automatically as soon as it is inserted.

Do not display last user name in logon screen - Enabled

Prevents the name of the last successful logon user from being displayed. This prevents a malicious user from acquiring it.

LAN Manager Authentication Level - Send NTLMv2 response only\refuse LM & NTLM

Only accepts NTLMv2 authentication. This is ideal for maximum security. For NTLMv2, password-derived keys are 128-bit encrypted.

Message text for users attempting to log on – Not defined

Not applicable

Message title for users attempting to log on – Not defined

Not applicable

Number of previous logons to cache (in case domain controller is not available) - 0 Logons

Not applicable. A value of 0 disables this setting.

Prevent system maintenance of computer account password - Disabled

Prevents the machine from requesting a weekly computer account password change.

Prevent users from installing printer drivers - Enabled

Enabled to prevent users form installing print drivers.

Prompt user to change password before expiration – 14 days

Not applicable

Recovery Console: Allow automatic administrative logon - Disabled

Requires the Administrator password to be provided when utilizing the Recovery Console. This is a must to maintain secure authenticated access to the workstation.

Recovery Console: Allow floppy copy and access to all drives and all folders – Disabled

Disables various Recovery Console environmental variables that are allowed very unrestrictive access to files, folders, and media on the machine.

Rename administrator account – Not defined

Renaming the Administrator account is critical to protecting against malicious user attacks. This is not defined in this template and is left to the Administrator to rename it. If it was set in this template, a malicious user would use this setting as well.

Rename guest account – Not defined

Similar to the Administrator account, protecting the guest account is critical as a malicious user could also target it.

Restrict CD-ROM access to locally logged-on user only – Enabled

Only allows interactive logon users to access the CD-ROM and not remote users

Restrict floppy access to locally logged-on user only – Enabled

Only allows interactive logon users to access the floppy and not remote users.

Secure channel: Digitally encrypt or sign secure channel data (always) – Disabled

Not applicable.

Secure channel: Digitally encrypt secure channel data (when possible) – Enabled

Not applicable

Secure channel: Digitally sign secure channel data (when possible) – Enabled

Not applicable

Secure channel: Require strong (Windows 2000 or later) session key – Disabled

Not applicable
Secure system partition (for RISC platforms only) – Not defined

Not applicable

Send unencrypted password to connect to third-party SMB servers - Disabled

If enabled, SMB client connection will send clear text passwords to non-Microsoft SMB server.

Shut down system immediately if unable to log security audits – Enabled

Collecting and preserving security logs are critical; therefore shutting down the system for this reason is acceptable.

Smart card removal behavior – Lock Workstation

Not applicable

Strengthen default permissions of global system objects (e.g. Symbolic Links) – Enabled

The Discretionary Access Control List (DACL) for objects is stronger by only allowing non-Administrator accounts to read shared objects but not modify them

Unsigned driver installation behavior – Warn but allow installation

Not applicable

Unsigned non-driver installation behavior – Warn but allow installation

Produces a warning to the installer that the non-device software has not been certified.

Security options modifies the registry settings without using registry editor.This

helps to prevent unexpected results that might appear from editing the registry.One important change is restricting anonymous remote connections. This prevents connection to the system using “Null user account”. Setting LAN manager authentication level to use NTLMv2 makes it harder for hackers to crack passwords on the system using tools such as L0phtCrack.

Event Log

Maximum application log size - 4194240 kilobytes

Sets the application log file size to the maximum possible. Disk storage permitting, this setting is probably ideal as collecting all system logs is critical.

Maximum security log size - 4194240 kilobytes

Sets the security log file size to the maximum possible. Disk storage permitting, this setting is probably ideal as collecting all system logs is critical.

Maximum system log size - 4194240 kilobytes

Sets the system log file size to the maximum possible. Disk storage permitting, this setting is probably ideal as collecting all system logs is critical.

Restrict guest access to application log - Enabled

Prevents guests from accessing the application log.

Restrict guest access to security log - Enabled

Prevents guests from accessing the security log.

Restrict guest access to system log - Enabled

Prevents guests from accessing the system log.

Retain application log - Not defined

Determines how long the application log will be retained before being overwritten.

Retain security log - Not defined

Determines how long the security log will be retained before being overwritten.

Retain system log - Not defined

Determines how long the system log will be retained before being overwritten.

Retention method for application log - Manually

Determines what to do with application events when the application log is full.

Retention method for security log – Manually

Determines what to do with security events when the security log is full.

Retention method for system log – Manually

Determines what to do with system events when the system log is full.

Shut down the computer when the security audit log is full - Enabled

Log file size is set to maximum value to gather as much data as possible. Guest users are not allowed to view Event logs for application, security or system. Logs are manually cleared to ensure that logs are not automatically destroyed. System will shut down when log files are full. These protect the system and preserve the logs if a major event happens.

Restricted Groups

This allows administrator to control the membership of groups. NSA template provides for only Power Users group and restrict this group to no members. Power Users is a sensitive group since it possesses most administrative privileges with some restrictions. This will help to prevent users from elevating their priviledge to Power Users Group through various hacks and attack tools.

System Services

This allows for the configuration of system services such as server services, smart card services etc. Services such as these can have the startup mode configured as either automatic, manual, or disabled. Permission of each service can be configured to permit or deny users the ability to modify the status of a service. Since system services are environment and application specific, they were not configured in this template. Unnecessary services should be disabled as they may be vulnerable to buffer overflow or denial of service (DoS) attacks.

Registry

This section provides the ability to modify permissions of certain registry settings. This can prevent unauthorised modification by users other than the

Administrator.

File System

This template modifies security permissions on the %SystemDrive%, %SystemDirectory%, %SystemRoot%, and %ProgramFiles% directory structures and some of their respective directories and files contained in them. The settings protect the system from unauthorized access to certain directories and files that contain sensitive configuration, system log, and authentication data such as account passwords.

5. Apply, Test, and Evaluate the Template

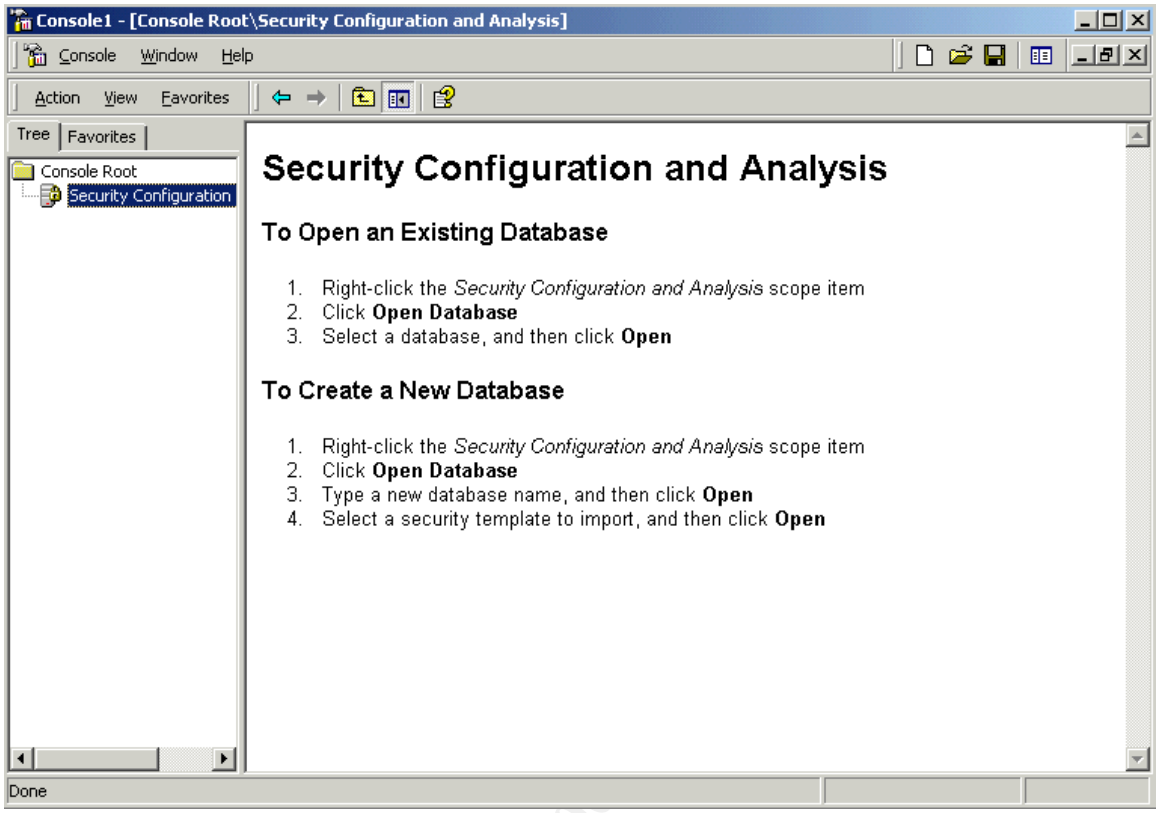
5.1. Apply The Template

Administrator on each system must perform the process of applying the template using the Microsoft Management Console. This includes modification to the template at a later date. This is due to restrictions placed on the system to prevent from being compromised remotely.

The steps taken to perform a security analysis using National Security Administration of the United States of America (NSA) workstation security template are as follows

- Copy or download the W2K_workstation.inf file to C:\template on the system.
- Open Microsoft Management Console by typing “mmc” in the “run” box.
- From the taskbar select “Console” then “Add/Remove Snap-in”.
- 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

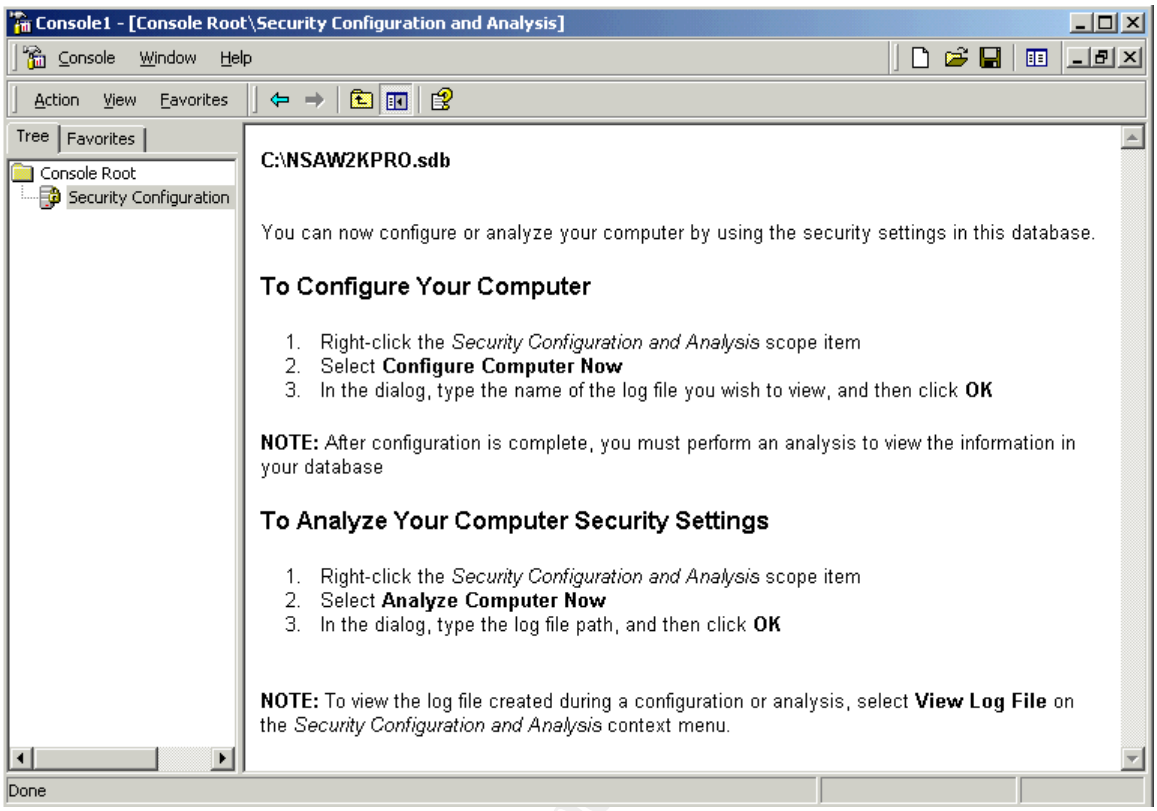
When Selecting “Security Configuration and Analysis” instructions will be provided in the main window detailing how to use the snap-in to analyze and configure the system. Refer to the next page.



Security Configuration And Analysis

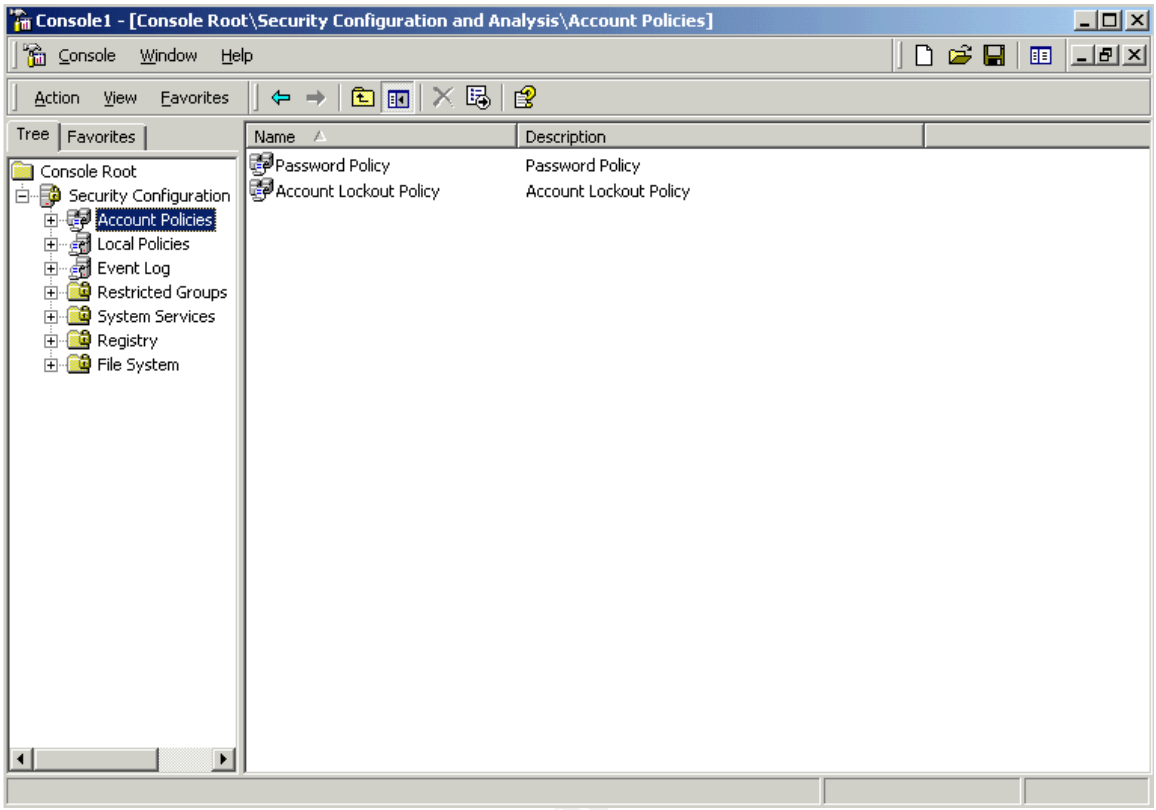
To load the NSA template, do the following

- 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"
- Browse to C:\template 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.



The template will be used to analyze the system security settings, to do that

- Right Click on the database node and select “Analyze Computer now”.
- A window will open prompting for the error log file path, enter C:\NSAW2KPRO.log and 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.

Policy	Database Setting	Computer Setting
Enforce password history	24 passwords reme...	0 passwords remem...
Maximum password age	90 days	42 days
Minimum password age	1 days	0 days
Minimum password length	12 characters	0 characters
Passwords must meet complexity r...	Enabled	Disabled
Store password using reversible e...	Disabled	Disabled

After reviewing the changes to be made to the system, it may be necessary to modify some of the settings.

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 C:\NSAW2KPRO.log and then click “OK”.

5.2. Test The Template's Security Settings

Account Policy Security Setting Test 1

Password Policy

Password must meet complexity requirements - Enabled

- Logon to console as Administrator.
- Launch Computer Management and right click Users to bring up New User dialog box.
- Attempt to create User name "sans" with password of "defgefghij1234"

Password fails to meet complexity requirements

Failure to Meet Minimum Password Length

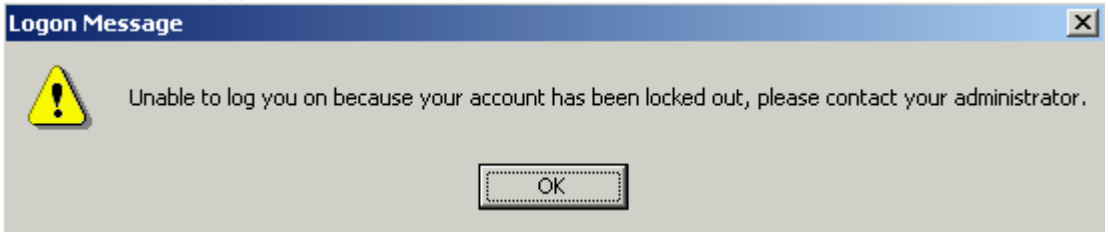
Account Policy Security Setting Test 2

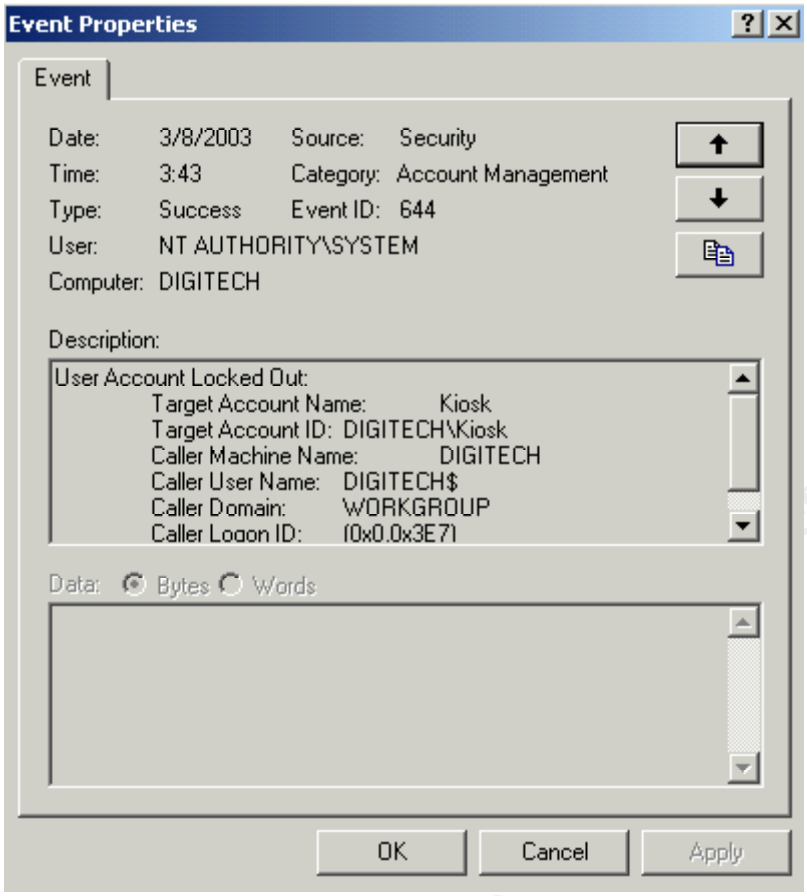
Account Lockout Policy

Account lockout threshold – 3 invalid logon attempts

- Logon as "kiosk" and enter incorrect password.
- Repeat incorrect password entry 3 times

Account is locked out after three invalid password attempts





Account Locked Out After 3 Invalid Password Entry

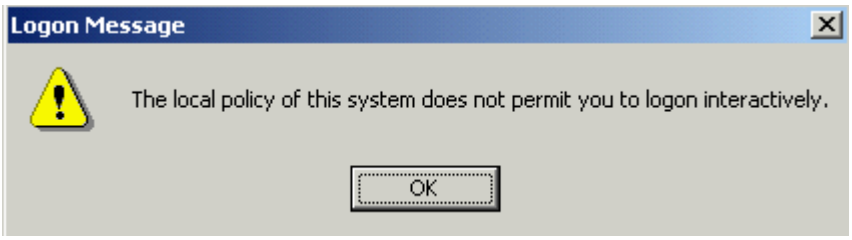
Local Policy Security Setting Test

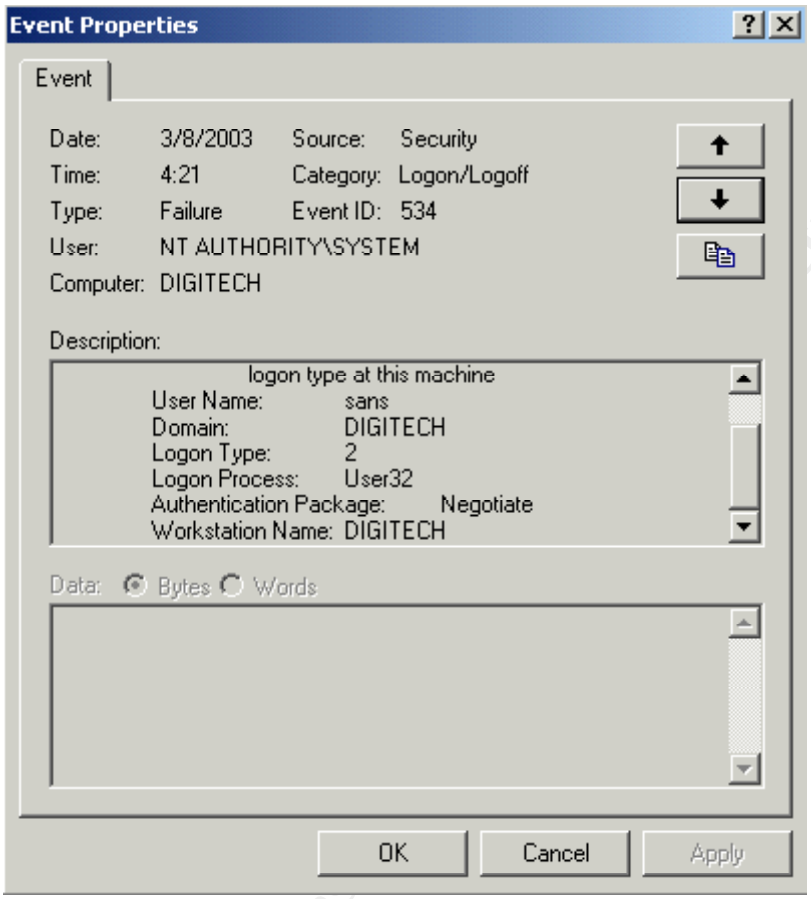
<u>User Rights Policy</u>

Logon on locally – Administrators, Users

- Logon as Administrator.
- Launch Computer Management and right click Users to bring up New User dialog box.
- Create new user "sans"
- Remove "sans" from Users group and make user "sans" a member of "Kiosk Users".
- Logout as Administrator.
- Logon as "sans".

User "sans" is not permitted to logon locally





Failure of User Account belonging to Kiosk Users group to Logon Locally

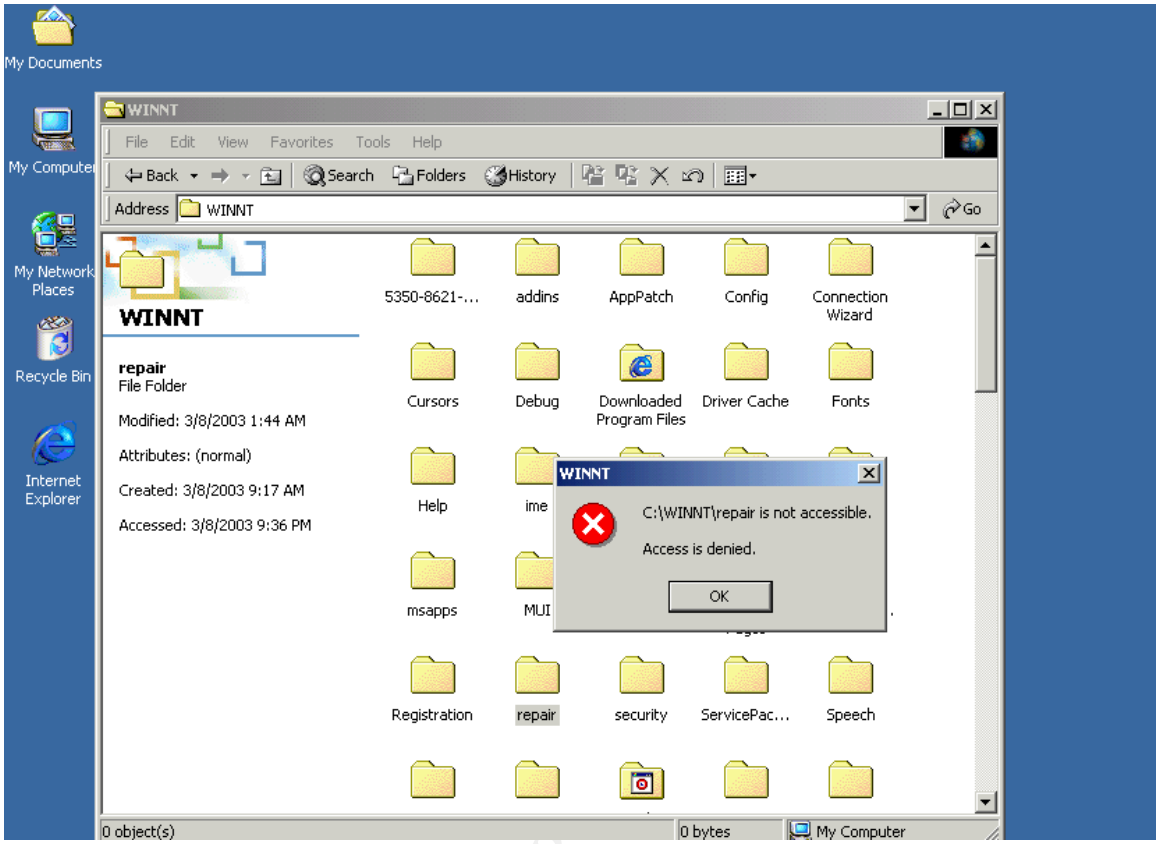
File System Security Setting Test

<u>File System</u>

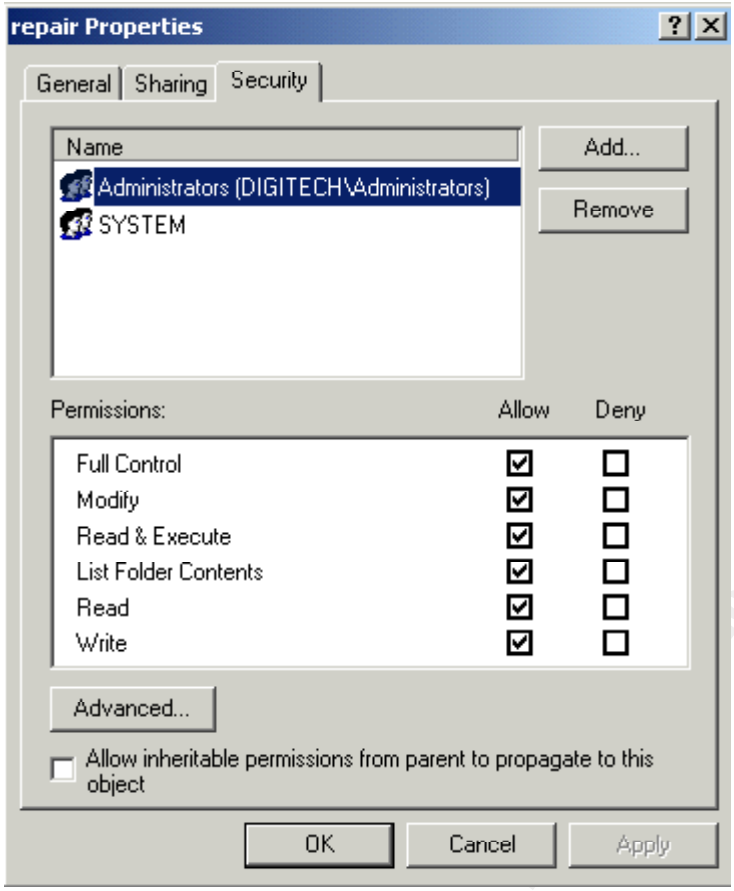
Access to %SystemRoot%\repair directory – Administrators, System

- Logon as "kiosk".
- Launch Windows Explorer and click on C:\WINNT\repair folder.

User "kiosk" is not permitted to access to the C:\WINNT\repair folder



Failure to access C:\WINNIT\Repair directory



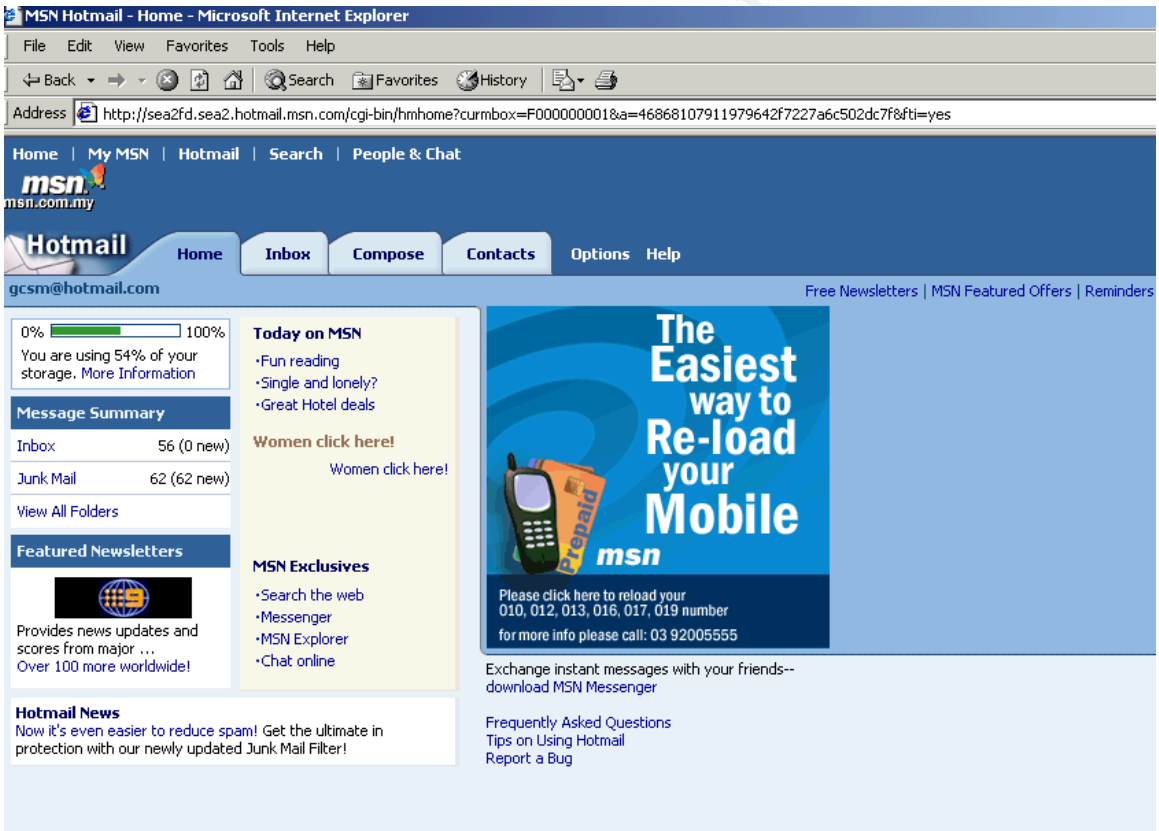
Repair Directory Security Properties

5.3. Test the System's Functionality

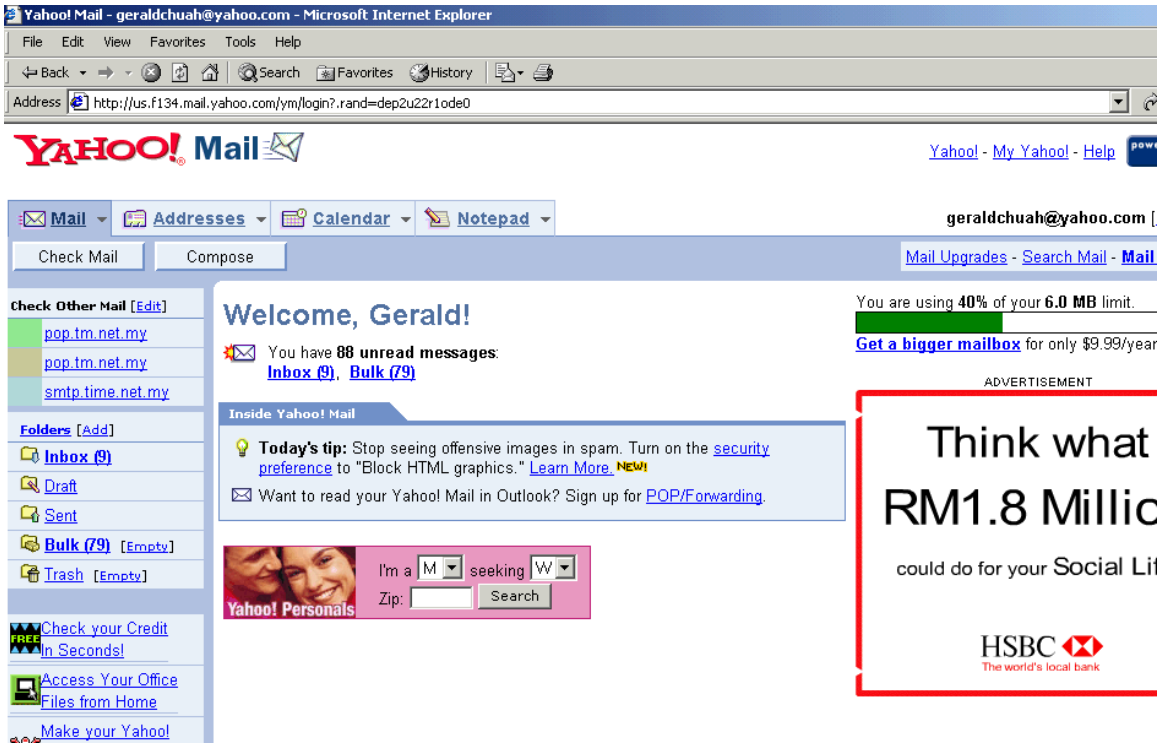
Able to connect to secure Internet Mail sites

- Login as “kiosk”
- Launch Inernet Explorer
- Logon to http://www.hotmail.com
- Read e-mails and delete junk e-mails
- Logoff http://www.hotmail.com
- Logon to http://mail.yahoo.com
- Read e-mails and delete junk e-mails
- Logoff http://mail.yahoo.com
- Close Internet Explorer

Able to logon, read and delete e-mails. No errors detected. Web connectivity functioned as expected



Able to connect to Hotmail



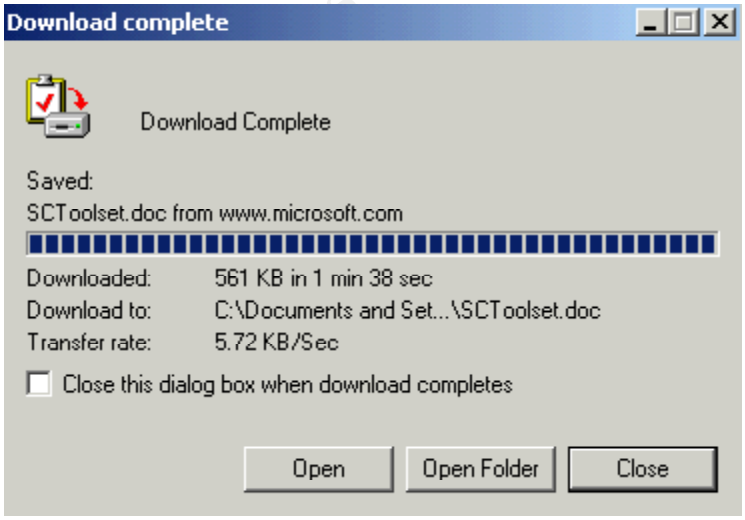
Able to connect to Yahoo mail

<u>Able to download files from Internet</u>

- Login as "kiosk"
- Launch Inernet Explorer
- Type the Internet Address http://www.microsoft.com/windows2000
- Click on Technical Resources, How it works

- Click on Security Configuration Tool Set
- Click on SCToolset.doc to download
- Close Internet Explorer

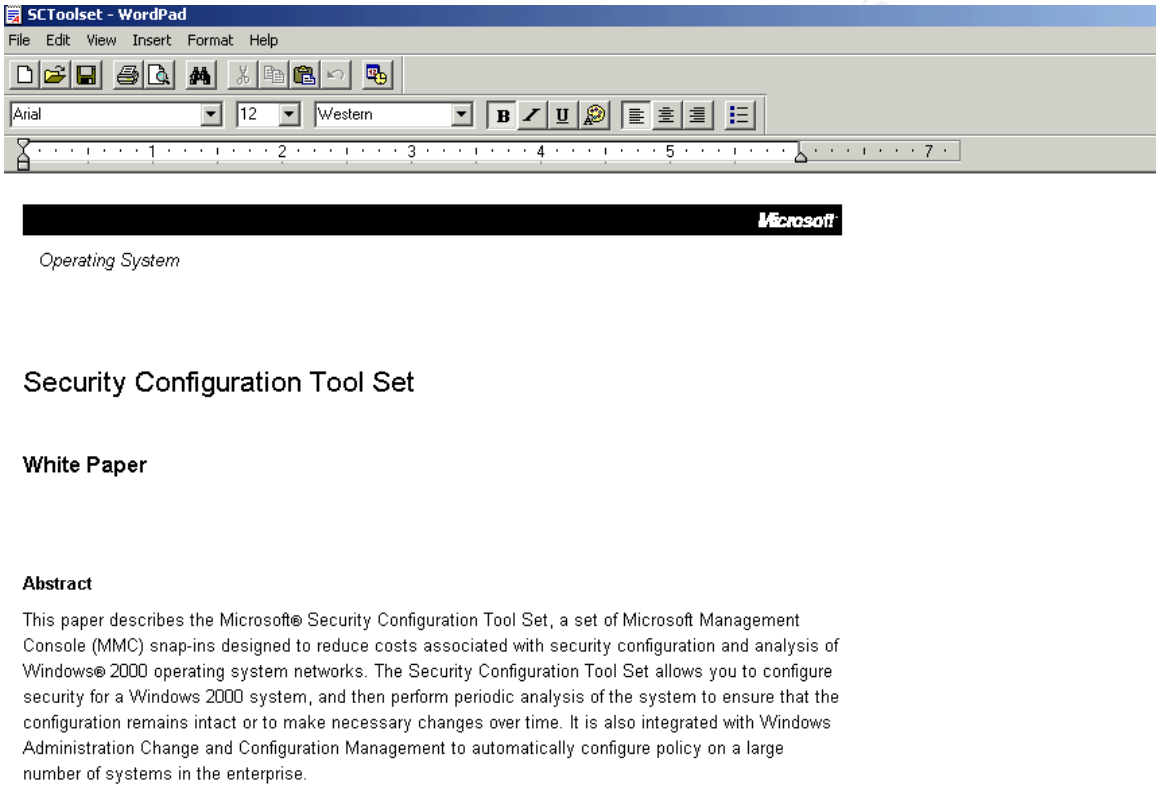
Able to download files to C:\document and settings\Kiosk folder. No errors detected



Downloaded SCToolset.doc file to C:\documents and settings\kiosk folder
Able to launch default applications

- Login as "kiosk"
- Launch WordPad
- Click File, Open, select SCToolset.doc
- Browse through the document
- Close WordPad.

Able to launch WordPad and read documents.

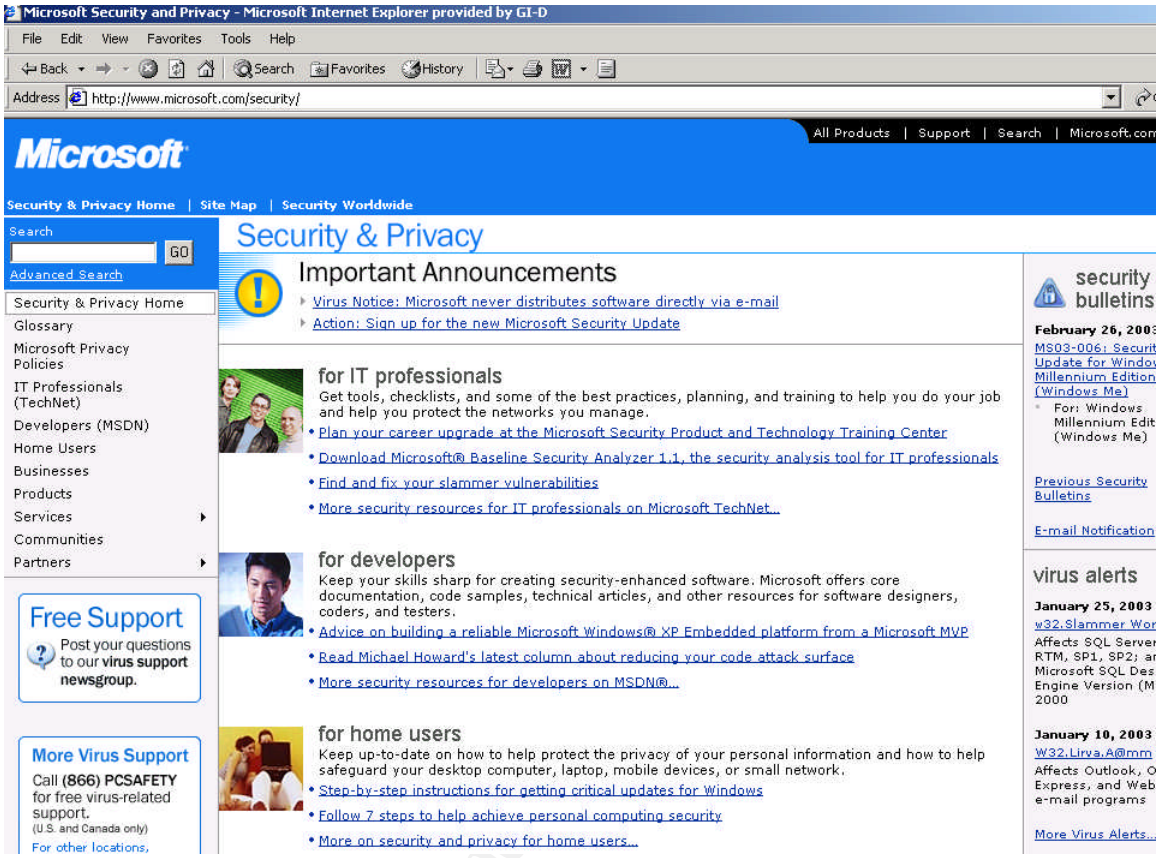


Able to open documents

Able to connect to Public internet sites

- Login as "kiosk"
- Launch Inernet Explorer
- Type the Internet Address http://www.microsoft.com/security
- Close Internet Explorer

Able to browse Public sites No errors detected.



Able to access Public site – http://www.microsoft.com/security

5.4. Evaluate the Template

Default Security Provided by the Template

The default security provided by the w2k_workstation.inf template provides an acceptable starting point for hardening the Windows 2000 operating system for business workstation that acts as a kiosk machine. But as stated in the documentation by the NSA, several sections require customisation based on the environment where the template is to be used.

Based on testing and research, it is necessary not only to customized the required sections but to change the number of settings. Settings that are not appropriate and need to be revised for a kiosk environment are as follows

Account Policy
Password Policy

Enforce password history – Not defined

Maximum password age – Not defined

Changing this will also change Minimum password age to Not defined

Minimum password length – Not defined

This is necessary because "kiosk" is the only account created and allowed for users to access the system. This will be an annoyance to Administrator account only during intial deployment.

Local Policy
User Rights Assignment

Access this computer from the network – Administrators

This will prevent users from accessing the system remotely.

Log on locally – Administrators, Kiosk Users

This will ensure only "kiosk" account other than the administrator is used to access the system. "Kiosk" account will be removed from Users group and added to Kisok Users group.

Shut down system – Administrators

This will prevent Kiosk Users from rebooting the system

Security options
Rename administrator account – Root

Administrator account is a target for hackers. Changing this will provide some security to the Administrator account. Create a new administrator account by editing sceregvl.ing file as described in NSA Guide to Securing Microsoft Windows 2000 Group Policy: Security Configuration Tool Set on page 50 in the section Adding an Entry to Security Options. This will act as a decoy to warn administrators that hacking attempts are attempted.

Rename guest account – Me

Rename this account to prevent hackers from targeting the default guest account. As an additional precaution, disable this guest account. Create a new guest account by editing sceregvl.ing file as described in NSA Guide to Securing Microsoft Windows 2000 Group Policy: Security Configuration Tool Set on page 50 in the section Adding an Entry to Security Options. This will act as a decoy to warn administrators that hacking attempts are attempted

Restricted Groups

"Kiosk Users" group is to be added to the restricted group and "kiosk" account added as member of this group. This is to ensure restrictions apply to the group as well as the account. The Power Users group should be removed, as there is no requirement for this. The system only supports Administrators

System Services

The template made no changes to system services configuration. As noted in the NSA documentation for this template, this was not done since tuning services is environment and system specific. It is recommended to disable any unnecessary services that are not required as they take up system resources and can potentially open holes into the operating system. Consideration should be given to disabling the following services:

Task Scheduler
Remote Registry
Remote access connection
Alerter
Computer Browser
DHCP Client
Distributed Link Tracking Client

Distributed Transaction Coordinator
DNS Client
Fax Service
Indexing Service
Internet Connection Sharing
Messenger
NetMeeting Remote Desktop Sharing
Network DDE
Network DDE DSDM
Print Spooler
QoS RSVP
Remote Access Auto Connection Manager
Remote Access Connection Manager
Remote Registry Service
Removable Storage
Run as a Service
Smart Card
Smart Card Helper
Task Scheduler
TCP/IP NetBios Helper Service
Telephony
Telnet
Uninterruptible Power Supply
Windows Time
Workstation

A more secure solution is to completely remove (uninstall) any unnecessary services identified above which would prevent them from ever being started. Kisok user group was restricted from makng any changes to the services on the system

File System

Modification needed to be made to prevent “Kisok user” group from executing ftp.exe, tftp.exe, mmc.exe, command.com and cmd.exe. The entire “kiosk” users “documents and settings” folder is set to deny write permissions to prevent “kiosk user” group from making any changes.

Impact of Template

As observed in the testing, the default template did not adversely affect any application functionality or user accessibility to the system. Use of Internet Explorer, default applications like WordPad displayed no anomalies or generated any errors.

6. Conclusion

There is considerable time spent to change the configuration of the template to increase the security of the system. But it helped reduce the vast amount of time in implementing them.

Even with the modified template, it is still not enough to secure the system as the whole process of hardening the system involves base installation, patching, hardening and template application. Some aspects of hardening will need to be revisited as Windows is the most popular target for hackers.

Some issues that cannot be addressed by the template include:

- Internet Explorer Settings like history information, browser default page and etc. This could be manipulated by the user.
- System desktop and many other settings could be manipulated by users. This also include many of the executable files.

It would be possible to apply Local Computer Group Policy to disable all of these and to explore the possibility of using the Internet Explorer Administration Kit to restrict the features of Internet Explorer.

7. References

1. Haney, Julie M., Guide to Securing Microsoft Windows 2000 Group Policy: Security Configuration Tool Set, Version 1.1.1, National Security Agency, URL: http://nsa2.www.conxion.com/win2k/guides/w2k-3.pdf, July 22, 2002

2. Security hotfixes by service pack at the Technet Security Bulletin Search http://www.microsoft.com/technet/security/current.asp

3. Microsoft Technet "HFNetChk" http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/tools/hfnetchk.asp

4. See What's New in HFNetChk 3.86 http://hfnetchk.shavlik.com/default.asp

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

6. Brian Stewart, The NSA W2K Workstation Template, http://www.giac.org/practical/Brian_Stewart_GCWN.doc Oct 2002

8. Appendix A w2k_workstation.inf Template

```
; (c) Microsoft Corporation 1997-2000
;
; Security Configuration Template for Security Configuration Editor
;
; Template Name:       W2k Workstation.INF
; Template Version:    05.00.DR.0000
;
; Revision History
; 0000  -          Original
; May 2001 - SNAC version 1.01a
; November 2001 -
;          Changed the line "RequireLogonToChangePassword = 1" to
;          "RequireLogonToChangePassword = 0" under the [System Access]
;          section. This line is an artifact from Windows NT 4.0 templates and could have
;          adverse effects on a user's ability to change password at first logon. If you have
;          experienced this problem, please reapply this corrected inf file, or, via a
;          text editor, create and apply an inf file with only the following lines:
;          [Unicode]
;          Unicode=yes
;          [System Access]
;          RequireLogonToChangePassword = 0

;
;          NOTE: This setting does NOT appear when the template file is viewed graphically in
;          the MMC.
;
; July 2002 -
;          In the Registry section, corrected the
;          MACHINE\System\CurrentControlSet\Control\Wmi\Security to grant Administrators Full
;          Control on the key and subkeys

[Unicode]
Unicode=yes
[System Access]
MinimumPasswordAge = 1
MaximumPasswordAge = 90
MinimumPasswordLength = 12
PasswordComplexity = 1
PasswordHistorySize = 24
LockoutBadCount = 3
ResetLockoutCount = 15
LockoutDuration = 15
RequireLogonToChangePassword = 0
ClearTextPassword = 0
[System Log]
MaximumLogSize = 4194240
AuditLogRetentionPeriod = 2
RetentionDays = 7
RestrictGuestAccess = 1
[Security Log]
MaximumLogSize = 4194240
```

```
AuditLogRetentionPeriod = 2
RetentionDays = 7
RestrictGuestAccess = 1
[Application Log]
MaximumLogSize = 4194240
AuditLogRetentionPeriod = 2
RetentionDays = 7
RestrictGuestAccess = 1
[Event Audit]
AuditSystemEvents = 3
AuditLogonEvents = 3
AuditObjectAccess = 2
AuditPrivilegeUse = 2
AuditPolicyChange = 3
AuditAccountManage = 3
AuditProcessTracking = 0
AuditDSAccess = 0
AuditAccountLogon = 3
CrashOnAuditFull = 1
[Version]
signature="$CHICAGO$"
Revision=1
[Privilege Rights]
seassignprimarytokenprivilege =
seauditprivilege =
sebackupprivilege = *S-1-5-32-544
sebatchlogonright =
sechangenotifyprivilege = *S-1-5-32-545
secreatepagefileprivilege = *S-1-5-32-544
secreatepermanentprivilege =
secreatetokenprivilege =
sedebugprivilege =
sedenybatchlogonright =
sedenyinteractivelogonright =
sedenynetworklogonright =
sedenyservicelogonright =
seenabledelegationprivilege =
seincreasebasepriorityprivilege = *S-1-5-32-544
seincreasequotaprivilege = *S-1-5-32-544
seinteractivelogonright = *S-1-5-32-544,*S-1-5-32-545
seloaddriverprivilege = *S-1-5-32-544
selockmemoryprivilege =
semachineaccountprivilege =
senetworklogonright = *S-1-5-32-544,*S-1-5-32-545
seprofilesingleprocessprivilege = *S-1-5-32-544
seremoteshutdownprivilege = *S-1-5-32-544
serestoreprivilege = *S-1-5-32-544
sesecurityprivilege = *S-1-5-32-544
seservicelogonright =
seshutdownprivilege = *S-1-5-32-544,*S-1-5-32-545
sesyncagentprivilege =
sesystemenvironmentprivilege = *S-1-5-32-544
sesystemprofileprivilege = *S-1-5-32-544
sesystemtimeprivilege = *S-1-5-32-544
```

```
setakeownershipprivilege = *S-1-5-32-544
setcbprivilege =
seundockprivilege = *S-1-5-32-544,*S-1-5-32-545
[Group Membership]
*S-1-5-32-547__Memberof =
*S-1-5-32-547__Members =
[Registry Keys]
"MACHINE\SYSTEM\CurrentControlSet\Services\SNMP\Parameters\ValidCommunities",2,"D:PA
R(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)"
"MACHINE\SYSTEM\CurrentControlSet\Services\SNMP\Parameters\PermittedManagers",2,"D:P
AR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)"
"MACHINE\SOFTWARE\Microsoft\OS/2 Subsystem for
NT",2,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)"
"machine\software",2,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)(A;CI;KR;;;BU)"
"machine\software\microsoft\netdde",2,"D:PAR(A;CI;KA;;;BA)(A;CI;KA;;;SY)"
"machine\software\microsoft\protected storage system provider",1,"D:AR"
"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)"
"machine\software\microsoft\windows\currentversion\group
policy",0,"D:PAR(A;CI;KA;;;BA)(A;CI;KR;;;AU)(A;CI;KA;;;SY)"
"machine\software\microsoft\windows\currentversion\installer",0,"D:PAR(A;CI;KA;;;BA)(A;CI;KA;;;
SY)(A;CI;KR;;;BU)"
"machine\software\microsoft\windows\currentversion\policies",0,"D:PAR(A;CI;KA;;;BA)(A;CI;KR;;;
AU)(A;CI;KA;;;SY)"
"machine\system",2,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)(A;CI;KR;;;BU)"
"machine\system\clone",1,"D:AR"
"machine\system\controlset001",0,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)(A;CI;KR
;;;BU)"
"machine\system\controlset002",0,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)(A;CI;KR
;;;BU)"
"machine\system\controlset003",0,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)(A;CI;KR
;;;BU)"
"machine\system\controlset004",0,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)(A;CI;KR
;;;BU)"
"machine\system\controlset005",0,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)(A;CI;KR
;;;BU)"
"machine\system\controlset006",0,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)(A;CI;KR
;;;BU)"
"machine\system\controlset007",0,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)(A;CI;KR
;;;BU)"
"machine\system\controlset008",0,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)(A;CI;KR
;;;BU)"
"machine\system\controlset009",0,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)(A;CI;KR
;;;BU)"
"machine\system\controlset010",0,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)(A;CI;KR
;;;BU)"
"machine\system\currentcontrolset\control\securepipeservers\winreg",2,"D:PAR(A;CI;KA;;;BA)(A;
;KR;;;BO)(A;CI;KA;;;SY)"
"machine\system\currentcontrolset\control\wmi\security",2,"D:P(A;CI;GR;;;BA)(A;CI;GA;;;SY)(A;C
I;GA;;;CO)"
"machine\system\currentcontrolset\enum",1,"D:PAR(A;CI;KA;;;BA)(A;CI;KR;;;AU)(A;CI;KA;;;SY)"
"machine\system\currentcontrolset\hardware
profiles",0,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)(A;CI;KR;;;BU)"
"users\.default",2,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)(A;CI;KR;;;BU)"
```

```
"users\.default\software\microsoft\netdde",2,"D:PAR(A;CI;KA;;;BA)(A;CI;KA;;;SY)"
"users\.default\software\microsoft\protected storage system provider",1,"D:AR"
"CLASSES_ROOT",2,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)(A;CI;KR;;;BU)"
"MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\AsrCommands",2,"D:PAR(A;CI;KA;;;BA)(A;CI;CCDCLCSWRPSDRC;;;BO)(A;
CIIO;KA;;;CO)(A;CI;KA;;;SY)(A;CI;KR;;;BU)"
[Registry Values]
machine\software\microsoft\driver signing\policy=3,1
machine\software\microsoft\non-driver signing\policy=3,1
machine\software\microsoft\windows nt\currentversion\setup\recoveryconsole\securitylevel=4,0
machine\software\microsoft\windows nt\currentversion\setup\recoveryconsole\setcommand=4,0
machine\software\microsoft\windows nt\currentversion\winlogon\allocatecdroms=1,1
machine\software\microsoft\windows nt\currentversion\winlogon\allocatedasd=1,0
machine\software\microsoft\windows nt\currentversion\winlogon\allocatefloppies=1,1
machine\software\microsoft\windows nt\currentversion\winlogon\cachedlogonscount=1,0
machine\software\microsoft\windows nt\currentversion\winlogon\passwordexpirywarning=4,14
machine\software\microsoft\windows nt\currentversion\winlogon\scremoveoption=1,1
machine\software\microsoft\windows\currentversion\policies\system\disablecad=4,0
machine\software\microsoft\windows\currentversion\policies\system\dontdisplaylastusername=4,
1
machine\software\microsoft\windows\currentversion\policies\system\shutdownwithoutlogon=4,0
machine\system\currentcontrolset\control\lsa\auditbaseobjects=4,1
machine\system\currentcontrolset\control\lsa\crashonauditfail=4,1
machine\system\currentcontrolset\control\lsa\fullprivilegeauditing=3,1
machine\system\currentcontrolset\control\lsa\lmcompatibilitylevel=4,5
machine\system\currentcontrolset\control\lsa\restrictanonymous=4,2
machine\system\currentcontrolset\control\print\providers\lanman print
services\servers\addprinterdrivers=4,1
machine\system\currentcontrolset\control\session manager\memory
management\clearpagefileatshutdown=4,1
machine\system\currentcontrolset\control\session manager\protectionmode=4,1
machine\system\currentcontrolset\services\lanmanserver\parameters\autodisconnect=4,30
machine\system\currentcontrolset\services\lanmanserver\parameters\enableforcedlogoff=4,1
machine\system\currentcontrolset\services\lanmanserver\parameters\enablesecuritysignature=4
,1
machine\system\currentcontrolset\services\lanmanserver\parameters\requiresecuritysignature=4
,0
machine\system\currentcontrolset\services\lanmanworkstation\parameters\enableplaintextpassw
ord=4,0
machine\system\currentcontrolset\services\lanmanworkstation\parameters\enablesecuritysignatu
re=4,1
machine\system\currentcontrolset\services\lanmanworkstation\parameters\requiresecuritysignat
ure=4,0
machine\system\currentcontrolset\services\netlogon\parameters\disablepasswordchange=4,0
machine\system\currentcontrolset\services\netlogon\parameters\requiresignorseal=4,0
machine\system\currentcontrolset\services\netlogon\parameters\requirestrongkey=4,0
machine\system\currentcontrolset\services\netlogon\parameters\sealsecurechannel=4,1
machine\system\currentcontrolset\services\netlogon\parameters\signsecurechannel=4,1
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AutoAdminLogon=4,0
MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoDriveTypeAutoRun=
4,255
[Profile Description]
Description=NSA Enhanced Security Settings for Windows 2000 Professional workstation
[File Security]
```

```
"%SystemDrive%\Program Files\Resource Pro Kit",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemRoot%\security",2,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)"
"%SystemDrive%\Documents and Settings\Default
User",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)"
"%SystemDrive%\ntldr",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemDrive%\config.sys",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)
"
"%SystemDrive%\ntdetect.com",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemDrive%\boot.ini",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemDrive%\autoexec.bat",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;
BU)"
"%SystemRoot%\Offline Web Pages",1,"D:(A;OICI;GA;;;WD)"
"%SystemDrive%\Documents and Settings\All
Users\Documents\DrWatson\drwtsn32.log",2,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;
FA;;;SY)(A;OICI;0x1301bf;;;BU)"
"%SystemRoot%\$NtServicePackUninstall$",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"c:\boot.ini",2,"D:PAR(A;;FA;;;BA)(A;;FA;;;SY)"
"c:\ntdetect.com",2,"D:PAR(A;;FA;;;BA)(A;;FA;;;SY)"
"c:\ntldr",2,"D:PAR(A;;FA;;;BA)(A;;FA;;;SY)"
"c:\ntbootdd.sys",2,"D:PAR(A;;FA;;;BA)(A;;FA;;;SY)"
"c:\autoexec.bat",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)"
"c:\config.sys",2,"D:PAR(A;;FA;;;BA)(A;;FA;;;SY)(A;;0x1200a9;;;BU)"
"%ProgramFiles%",2,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)(A;OICI;0x120
0a9;;;BU)"
"%SystemRoot%",2,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)(A;OICI;0x1200
a9;;;BU)"
"%SystemRoot%\CSC",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemRoot%\debug",0,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)(A;OICI;0
x1200a9;;;BU)"
"%SystemRoot%\Registration",0,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)(A;OICI;FR;;;BU)"
"%SystemRoot%\repair",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemRoot%\Tasks",1,"D:AR"
"%SystemRoot%\Temp",2,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)(A;CI;0x1
00026;;;BU)"
"%SystemDirectory%",2,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)(A;OICI;0x1
200a9;;;BU)"
"%SystemDirectory%\appmgmt",0,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;B
U)"
"%SystemDirectory%\DTCLog",0,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)(A;
OICI;0x1200a9;;;BU)"
"%SystemDirectory%\GroupPolicy",0,"D:PAR(A;OICI;FA;;;BA)(A;OICI;0x1200a9;;;AU)(A;OICI;FA
;;;SY)"
"%SystemDirectory%\NTMSData",0,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemDirectory%\Setup",0,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)"
"%SystemDirectory%\ReinstallBackups",1,"D:P(A;OICI;GXGR;;;BU)(A;OICI;GXGR;;;PU)(A;OICI;
GA;;;BA)(A;OICI;GA;;;SY)(A;OICI;GA;;;CO)"
"%SystemDirectory%\repl",0,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)"
"%SystemDirectory%\repl\import",0,"D:PAR(A;OICI;FA;;;BA)(A;OICI;0x1301bf;;;RE)(A;OICI;FA;;;
SY)(A;OICI;0x1200a9;;;BU)"
"%SystemDirectory%\repl\export",0,"D:PAR(A;OICI;FA;;;BA)(A;OICI;0x1200a9;;;RE)(A;OICI;FA;;
;SY)(A;OICI;0x1200a9;;;BU)"
"%SystemDirectory%\spool\printers",2,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;S
Y)(A;CI;DCLCSWWPLO;;;BU)"
"%SystemDirectory%\config",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
```

```
"%SystemDirectory%\dllcache",2,"D:P(A;OICI;GA;;;BA)(A;OICI;GA;;;SY)(A;OICI;GA;;;CO)"
"%SystemDirectory%\ias",2,"D:P(A;OICI;GA;;;BA)(A;OICI;GA;;;SY)(A;OICI;GA;;;CO)"
"%SystemDrive%\Documents and
Settings",0,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)"
"%SystemDrive%\My Download
Files",2,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)(A;OICI;0x1201bf;;;BU)"
"%SystemDrive%\System Volume Information",1,"D:PAR"
"%SystemDrive%\Temp",2,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)(A;CI;DC
LCWP;;;BU)"
"%SystemDrive%\",0,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)(A;OICI;0x120
0a9;;;BU)"
"%SystemDrive%\IO.SYS",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)"
"%SystemDrive%\MSDOS.SYS",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;
BU)"
"%SystemRoot%\regedit.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemDirectory%\rcp.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemDirectory%\Ntbackup.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemDirectory%\rexec.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemDirectory%\rsh.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemDirectory%\regedt32.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemDrive%\Documents and
Settings\Administrator",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemDrive%\Documents and Settings\All
Users\Documents\DrWatson",2,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)(A;O
ICIIO;DCLCWP;;;BU)(A;OICI;CCSWWPLORC;;;BU)"
"%SystemDirectory%\secedit.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemRoot%\Debug\UserMode",0,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)(A;;CCDCWP;;;B
U)(A;OIIO;DCLC;;;BU)"
"%SystemDrive%\Documents and Settings\All
Users",0,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)"
```