SANS GIAC

GCNT CERTIFICATION PRACTICAL

JOHN M. MILLICAN

April 7, 2001

Assignment Overview

The objective of this paper is to provide an in-depth examination of how the automation tools provided with Windows 2000 can be used to facilitate the process of securing servers upon which it is installed.

Three areas will be focused upon: the Security Configuration and Analysis Tool set, the pre-defined security templates provided with Windows 2000, and the use of the Windows Script Host for security purposes.

With all the security features available in Windows 2000, it can be overwhelming to system administrators. The tools provided with Windows 2000 perform many valuable functions to assist administrators with these daunting tasks.

The security features of Windows 2000 are scattered throughout the system. System parameters are stored in the Registry. Resource access rights run throughout the file system and network resources. Services hide in the Computer Management MMC snap-in. The automation tools provide a central location to configure the majority of these security settings.

The automation tools also make it possible for the administrator to efficiently check the myriad settings. Without the assistance of these tools it would be very easy to overlook a critical configuration error that leaves a system wide open for abuse. The tools provide a distilled view to spot these shortcomings.

The tools assist with the adjustment of security settings by propagating policies throughout the system. This also reduces the possibility of human error.

In addition to establishing an initial security stance, the tools are helpful in auditing a system over the course of its life. Additional, they can be used for forensic analysis after a system has been compromised.

But perhaps the most important contribution of the automation tools is that they pass the collective knowledge of system experts to less knowledgeable administrators who are nonetheless charged with the responsibility of securing their companies' valuable resources. Merely by looking at the tree structure used by the Security Configuration and Analysis Tool provides an insight into the approach that the experts use to harden a system. As you drill down the tree, it is easy to appreciate details that need to be attended to. The Security Templates provided with Windows 2000 convey the best practices developed by the experts with specific settings to be used in varying circumstances.

However, all of these same features can be harmful if not applied properly. In the hands of a professional, a circular saw provides a substantial boost to the worker’s quality and productivity. But the same tool in the hands of a child can do great harm just as rapidly.

For this reason it is important to examine these tools to learn how they work, what their capabilities are, and what their shortcomings are. Only in this way can their full benefit be derived.

Security Configuration Tool Set

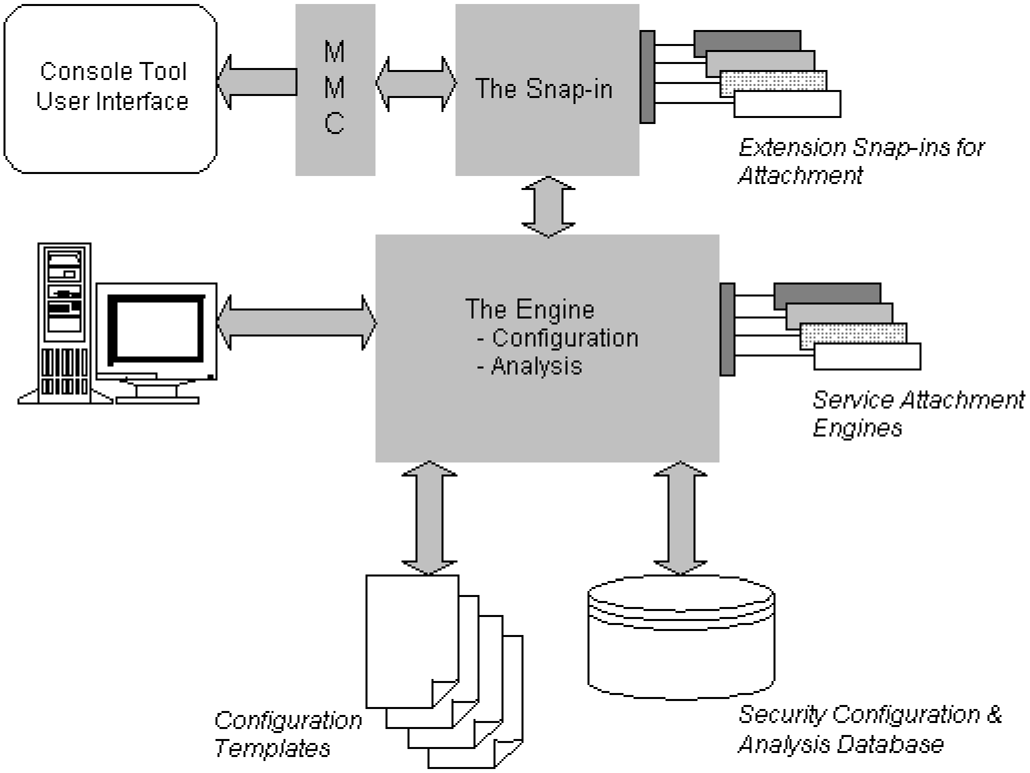
Overview

Originally released with Service Pack 4 of Windows NT, the Security Configuration Tool Set started the process of consolidating the security settings into a centralized location. With the introduction of Windows 2000, Microsoft has expanded its capabilities.

The Security Configuration Tool Set is comprised of the following components:

- Security Configuration Service
  The heart of the tool set, it runs on every Windows 2000 system providing the configuration and analysis capabilities used by the rest of the tool set.
- Setup Security
  This establishes the initial security configuration during system setup. It is rudimentary at the best.
- Security Configuration and Analysis Tool
  SCAT is a Microsoft Management Console snap-in that provides a central location for the definition of security settings, systems analysis, and saved configuration files. This tool is primarily used to manage the local computer it is installed on.
- Group Policy Security Extensions
  With the introduction of Active Directory in Windows 2000, Microsoft also extended the Security Configuration Tool Set to the Group Policy Object. This allows a security stance to be established on a domain, organizational unit or a specific computer. It is also more dynamic than SCAT because it is a part of Group Policy.
- Secedit.exe
  This is a command line interface providing access to a limited number of the tool set's features. It is useful for inclusion in scripts.

The following graphic taken from Microsoft's TechNet site provides an excellent illustration of the relationship of the components of the Security Configuration Tool Set.


Console Tool User Interface
M M C
The Snap-in
Extension Snap-ins for Attachment
The Engine
- Configuration
- Analysis
Service Attachment Engines
Configuration Templates
Security Configuration & Analysis Database

Security Configuration and Analysis Tool

The focus of this section will be on the Security Configuration and Analysis Tool (SCAT). SCAT provides a simple uniform graphical user interface (GUI) for defining configurations, saving them to files, and viewing security analysis data stored in the security analysis database. The interface uses the standardized context menus and views supported by Microsoft Management Console.

During a clean installation of Windows 2000, the initial settings are stored in the local computer policy database. SCAT comes with a set of pre-defined security templates. To implement the settings SCAT is executed, a template is imported, the settings of the template are compared to the computer's settings, adjustments are made to the template, the database settings are applied to the computer, and the settings are exported to act as a backup of the policy implemented.

The pre-defined templates are intended by Microsoft to be additive in nature. In other words as templates with tighter security settings are imported, the security stance of the computer increases. As will be shown in this paper, that is not entirely the case.

Pre-defined templates are provided for the different roles that a Windows 2000 computer can perform. These roles are workstation, server, compatible, and domain controller. All of the roles are self-explanatory except for the compatible role. This template is used to provide certified Windows 2000 applications the ability to run in the User context while allowing non-certified applications to run in the less secure Power Users context.

Security Policy Areas

SCAT divides security policy into five groupings called security areas: account policies; local policies; event logging; restricted groups; and system services, registry and file system.

Account Policy

Account policies apply to user accounts and cover three areas: password policy, account lockout policy, and Kerberos policy.

Password policy manages the settings for the number of passwords remembered, maximum and minimum password ages, minimum password length, and complexity requirements.

Account lockout policy establishes settings for account lockout duration, threshold and counter reset.

Local Policy

As the name implies, local policies are effective on the local computer. The areas covered are audit policy, user rights assignment and event logging. In conjunction with account policies, local policies are the heart of the system's security settings.

Audit policy determines which security events, successful or failed, are logged in the Security Log.

User rights assignment determines which users or groups have logon or task privileges on the computer.

Security options is a catchall bucket for settings dealing with digital signing of data, access to CD or floppy drives, driver installation and logon prompts.

Event Logging Policy

This policy area deals with settings pertaining to log size, user access rights to the system logs, retention length and rollover methods.

Since these settings are based on enterprise specific conditions such as transaction volume and backup intervals, it is virtually impossible for any specific settings to be recommended. Therefore, the primary value of this area is to make it visible for consideration.

Restricted Groups Policy

Restricted group policy ensures that group memberships are properly enforced. Any group or member not listed in the restricted group membership is removed. Additionally, there is a reverse membership option that removes the restricted group from any groups not specifically listed in the Members Of list.

System Services, Registry, and File System Policy

These security areas define the access permissions for users and groups to the file system, registry and system services. It can be used to manage read/write/delete/execute permissions, inheritance settings, auditing, and the startup properties of the system services.

Microsoft Security Templates Compared To SANS Windows 2000 Recommendations

The combination of SCAT and the Microsoft Security Templates represent a powerful management aid for administrators. However, without detailed knowledge of the settings, it can also provide a false sense of security.

With that in mind a thorough examination of each template and the changes they effect should be undertaken. To judge the effectiveness of the templates they should be measured against a high quality standard. The SANS Windows 2000 Step By Step was chosen for that purpose.

A clean installation of Windows 2000 Server was performed. After installation it was promoted to act as the Domain Controller. The pre-defined templates were applied in the following order: basicdc, securedc, and hisecdc. After each template was applied, each setting was examined to determine what changes had been made. Each setting was also compared to the SANS recommendations to determine how well the template met the standard.

The following represents the results of that examination.

Basicdc Security Template

Overview

The basicdc template is used to return a system to the default Windows 2000 security settings with the exception of user rights. Microsoft justifies that exception by stating that would not be appropriate to override settings that application programs may have made. Since no applications were installed after the clean installation, the resulting user rights also reflected Windows 2000's defaults.

Discrepancies between the base policies and the SANS recommendations are highlighted in yellow.

Template

Section	Description	Step By Step	Installed Settings
3.1.1	Account Policy		
	Enforce Password History	8 – 13 Passwords	1 Password
	Maximum Password Age	45 – 90 Days	42 Days
	Minimum Password Age	1 – 5 Days	0 Days
	Minimum Password Length	8 Characters	0 Characters
	Passwords must meet complexity requirements	Enabled	Disabled
	Store passwords using reversible encryption for all users in the domain	Disabled	Disabled
	Account Lockout Duration	4 Hours	Not Defined
	Account Lockout Threshold	5 Failed Attempts	0
	Reset Account Lockout Counter After	4 Hours	Not Defined
3.1.2	Local Policy		

Section	Description	Step By Step	Installed Settings
3.1.2.1	Audit Policy		
	Account Logon Events	Success, Failure	No Auditing
	Account Management	Success, Failure	No Auditing
	Logon Events	Success, Failure	No Auditing
	Object Access	Success, Failure	No Auditing
	Policy Change	Success, Failure	No Auditing
	Privilege Use	Success, Failure	No Auditing
	Process Tracking	Not Specified	No Auditing
	System Events	Success, Failure	No Auditing
3.1.2.2	User Rights		
	Access this computer from the network	Domain Users	Administrators, IWAM, IUSR, Authenticated Users, Everyone
	Act as part of the operating system	None	None

Section	Description	Step By Step	Installed Settings
	Add workstations to domain	Administrators	Authenticated Users
	Backup files and directories		Backup Operators, Administrators, Server operators
	Bypass traverse checking	Administrators, Server Operators and Backup Operators	Administrators, Authenticated Users, Everyone
	Change the system time	Administrators	Server operators, Administrators
	Create a page file	Domain Administrators	None
	Create a token object	None	None
	Create permanent shared objects		None
	Debug programs	None	Administrators
	Deny access to this computer from the network	Administrators	None
	Deny logon as a batch job	Not Specified	None

Section	Description	Step By Step	Installed Settings
	Deny logon as a service	Not Specified	None
	Deny logon locally	Not Specified	None
	Enable computer and user accounts to be trusted for delegation	Not Specified	Administrators
	Force shutdown from a remote system	Not Specified	Server Operators, Administrators
	Generate security audits	Not Specified	None
	Increase quotas	Not Specified	Administrators
	Increase scheduling	Administrators	Administrators
	Load and unload device drivers	Administrators	Administrators
	Lock pages in memory	None	None
	Logon as a batch job	None	IWAM, IUSR
	Logon as a service	None	None
	Logon locally	Administrators, Server Operators and Backup	Backup Operators, Print Operators, Server

Section	Description	Step By Step	Installed Settings
		Operators	Operators, Account Operators, Administrators
	Manage auditing and security logs	Administrators	Administrators
	Modify firmware environment values	Administrators, Server Operators and Backup Operators	Administrators
	Profile single process	Not Specified	Administrators
	Profile system performance	Not Specified	Administrators
	Remove computer from docking station	Not Specified	Administrators
	Replace a process level token	None	None
	Restore files and directories	Backup Operators	Backup Operators, Server Operators, Administrators
	Shutdown the server	Administrators and Server Operators	Backup Operators, Print Operators, Server Operators,

Section	Description	Step By Step	Installed Settings
			Account Operators, Administrators
	Synchronize directory service data	Not Specified	None
	Take ownership of files or other objects	Administrators	Administrators
3.1.2.3	Security Options		
3.1.2.3.1	Additional restrictions for anonymous connections	No Access Without Explicit Restrictions	None, Rely On Default Permissions
3.1.2.3.2	Allow Server Operators to Schedule Tasks	Disable	Not Defined
3.1.2.3.3	Allow System to be Shut Down Without Having to Log On	Enable only at sites with strong physical security	Disabled
3.1.2.3.4	Allowed to Eject Removable NTFS Media	Not Specified	Administrators
3.1.2.3.5	Amount of Idle Time Required Before Disconnecting Session	15 Minutes	15 Minutes

Section	**Description**	**Step By Step**	**Installed Settings**
3.1.2.3.6	Audit the Access of Global System Objects	Undefined or Disabled	Disabled
3.1.2.3.7	Audit Use of Backup and Restore Privilege	Enable	Disabled
3.1.2.3.8	Automatically Log Off Users When Logon Time Expires	Enable	Disabled/Enabled (Local)
3.1.2.3.9	Clear Virtual Memory Pagefile When System Shuts Down	Enable	Disabled
3.1.2.3.10	Digitally Sign Client Communication	When Possible	Always-Disabled When Possible-Enabled
3.1.2.3.11	Digitally Sign Server Communication	When Possible	Always-Disabled When Possible-Enabled
3.1.2.3.12	Disable CTRL+ALT+DEL Requirement for Logon	Disable	Disabled
3.1.2.3.13	Do Not Display Last User Name in Logon Screen	Enable	Disabled
3.1.2.3.14	LAN Manager	Send NTLMv2	Send LM and

Section	Description	Step By Step	Installed Settings
	Authentication Level	response only	NTLM responses
3.1.2.3.15	Message Text/Title for users attempting to Logon	Provide text after consulting with legal counsel	None
3.1.2.3.16	Number of Previous Logons to Cache	0	10
3.1.2.3.17	Prevent System Maintenance of Computer Account Password	Disable	Disabled
3.1.2.3.18	Prevent Users From Installing Print Drivers	Enable	Enabled
3.1.2.3.19	Prompt User to Change Password Before Expiration	14 Days	14 Days
3.1.2.3.20	Recovery Console: Allow Automatic Administrative Logon	Disable	Disabled
3.1.2.3.21	Recovery Console: Allow Floppy Copy and Access to All Drives and Folders	Disable	Disabled
3.1.2.3.23	Restrict the CD-ROM and Floppy drive access to locally	Enable	Disabled

Section	Description	Step By Step	Installed Settings
	logged on user only		
3.1.2.3.24	Secure the Netlogon Channel	Require strong (Windows 2000 or later) session key	Disabled
3.1.2.3.25	Send Unencrypted Password to Connect to Third-Party SMB Servers	Disable	Disabled
3.1.2.3.26	Shut Down System Immediately If Unable to Log Security Audits	Enable (with care)	Disabled
3.1.2.3.27	Configure Smart Card Removal Behavior	Lock the workstation	No Action
3.1.2.3.28	Configure Unsigned Driver Installation Behavior	Do not allow installation	Warn but allow installation
3.1.2.3.29	Configure Unsigned Non-Driver Installation Behavior	Warn but allow installation	Succeed silently
3.3.1.1	Maximum Log Size	Enough to last between full backups	512 KB
	Retention Period	Number of Days between	7 Days

Section	Description	Step By Step	Installed Settings
		full backups	
	Retention Method	By Days	By Days
3.3.2.1	WMI Control	Disable if not needed	Not Defined
3.3.2.3	Indexing Service	Disable if not needed	Not Defined

Analysis

Not that it should come as any great surprise, but that's a lot of yellow. The basicdc template provides very little in the way of security and falls substantially short of the SANS Step By Step recommendations.

Password security protections are minimal at best. The number of passwords remembered is too low. Combined with the fact that there is no minimum password age, the settings allow a user to easily retain the same, weak password indefinitely. There are also no minimum character or complexity requirements. Additionally, the system accepts the LanMan hashing mechanism that can be sniffed on the network and is trivial to crack with L0phtCrack. The SAM database is not encrypted and is accessible by the anonymous user. This makes it easy to obtain all of the domain's user names and password hashes which L0phtCrack can then parse in its entirety.

If that wasn't enough, there are no logon account protections in place. So even if the passwords could not be obtained using the methods outlined above, there is nothing to hinder a brute force logon attack.

The Account Policy area is intended to protect against these two types of attack. First, it allows for the requirement that passwords be long and complex. Second, it can be required that passwords be stored and transmitted in a secure manner. Third, it can require that users generate new passwords on a frequent basis so that an attacker will not have time using today's technology to brute force the password.

Additionally, there is no logging being done. A primary purpose of logging is to record anomalous activity. Doorknob rattling such as a brute force access attempts definitely fall into this category. So would attempts at privilege escalation and policy changes. Without logging these actions would go by unnoticed.

User rights are lax as well. Allowing the Administrator account to manage the server remotely extends all of the Administrator's powers throughout the network. With these settings it is possible to control the critical resources of the server from anywhere it can be reached with a TCP packet. This certainly makes it possible for an attacker who does not have physical access to the server to exploit the system nonetheless.

Since any authenticated user can add workstations to the domain, it is possible for users with limited system privileges to add a workstation without approval. This workstation would not have to have an approved security configuration. Its security stance may be even worse than that of the server, and it may have hardware that could circumvent security measures in place elsewhere on the network. For instance, a user or an attacker could bypass the corporate firewall if it was configured with a dial-in modem.

The pool of users allowed to logon locally is too wide. Users such as Print Operators do not need physical access to the server to perform their jobs. But granted that right, as this policy template does, it allows those relatively unprivileged users to run exploits such as GetAdmin to escalate their privileges.

Allowing too many users backup and restore rights exposes the system in a variety of ways. In the case of backup rights, loose privileges might give an otherwise unauthorized person the right to copy and remove valuable data from the site. Loose restore privileges could allow a malicious program to be copied onto the system.

Too many people are granted the right to shutdown the system locally. This could be used for something as simple as a denial of service attack, or it could be used to reboot to an alternative OS such as Linux that does not recognize Windows 2000 security mechanisms. Of course, maybe we should be happy that they do a clean shutdown instead of just pulling the plug.

This policy allows Server Operators the ability to schedule jobs. This right is dangerous because it could be used to run code in the System context that is among the most privileged in Windows 2000.

If user logon times are used on the system, there is nothing in these policies to stop a user from staying logged onto the system beyond their authorized hours. So while they may not be able to logon in the middle of the night when all the supervisors are gone, they can just remain on instead.

Should it ever be desired to prosecute someone for unauthorized use or access to the system, the lack of a logon warning would substantially weaken, if not cripple, the case.

Finally, the system's response to the installation of unsigned drivers is too lenient. Device drivers run in Windows 2000's highest security context - Kernel mode. The ability to install drivers not vouched for by a reputable source opens a large hole through which malicious programs can be passed.

Securedc Security Template

Overview

To address some of the concerns presented by the basicdc policies, Microsoft suggests that the securedc template be used. According to the Windows 2000 Help pages, "the secure templates implement recommended security settings for all security areas except files, folders, and registry keys."

Template

The following are the changes made by applying the securedc template. Differences between it and the SANS recommendations are highlighted in yellow.

Section	Description	Step By Step	Securedc Settings
3.1.1	Account Policy		
	Enforce Password History	8 – 13 Passwords	24 Passwords
	Minimum Password Age	1 – 5 Days	2 Days
	Minimum Password Length	8 Characters	8 Characters
	Passwords must meet complexity requirements	Enabled	Enabled
	Account Lockout Duration	4 Hours	30 Minutes
	Account Lockout Threshold	5 Failed Attempts	5
	Reset Account Lockout Counter After	4 Hours	30 Minutes
3.1.2	Local Policy		
3.1.2.1	Audit Policy		
	Account Logon Events	Success, Failure	Failure
	Account Management	Success, Failure	Success, Failure
	Logon Events	Success, Failure	Failure
	Object Access	Success, Failure	No Auditing

	Policy Change	Success, Failure	Success, Failure
	Privilege Use	Success, Failure	Failure
3.1.2.2	User Rights		
	Create a page file	Domain Administrators	Administrators
3.1.2.3	Security Options		
3.1.2.3.1	Additional restrictions for anonymous connections	No Access Without Explicit Restrictions	Do Not Allow Enumeration of SAM accounts and shares
3.1.2.3.2	Allow Server Operators to Schedule Tasks	Disable	Disabled
3.1.2.3.8	Automatically Log Off Users When Logon Time Expires	Enable	Enabled
3.1.2.3.14	LAN Manager Authentication Level	Send NTLMv2 response only	Send NTLM response only
3.1.2.3.23	Restrict the CD-ROM and Floppy drive access to locally logged on user only	Enable	Enabled
3.1.2.3.24	Secure the Netlogon Channel	Require strong (Windows 2000 or later) session key	Disabled

3.1.2.3.27	Configure Smart Card Removal Behavior	Lock the workstation	Force Logoff
3.1.2.3.28	Configure Unsigned Driver Installation Behavior	Do not allow installation	Do not allow installation
3.1.2.3.29	Configure Unsigned Non-Driver Installation Behavior	Warn but allow installation	Warn but allow installation
3.3.1.1	Maximum Log Size	Enough to last between full backups	Security Log Increased to 5MB

Analysis

The securedc template brings the configuration of the Windows 2000 domain controller closer to the SANS recommendations, but a lot of yellow remains.

This template significantly tightens account password policies by remembering 24 passwords and enforcing minimum password age, length and complexity. It also puts in place account lockout policies, but these are still more lenient than the SANS recommendations. As a result, brute force attacks at night are easier to conduct than they should be.

Auditing is also put in place, but again it does not meet SANS standards. While brute force logon attempts would now show up in the event logs, anomalous logons would not. If for instance a user's account is comprised, a logon outside of that user's normal usage hours would not be noticed because only failed logons are recorded. Also, successful yet inappropriate use of privileges would not be detected because again only failed privilege attempts would be logged.

The event auditing log sizes are not in line with SANS' recommendations, but it is impossible for any tool to state in advance what the sizes should be for your environment. This is because log size is dependent on many factors including the amount of activity on the system and backup intervals. That is why SANS recommends a way to determine the values rather than just specifying an arbitrary value.

Progress is also made in tightening user rights. The ability to create a page file is now limited to Administrators.

The system is protected from server operators by not allowing them to schedule tasks. This prevents them from being able to run a process in the System context.

Forcing logoff when the logon time expires protects the systems from curious users working outside of times when they would otherwise have supervisory oversight.

Anonymous connections can no longer enumerate the SAM database. But the "Do Not Allow Enumeration of SAM accounts and shares" still provides the "Network" group access to resources they require. The "Network" group includes all users currently accessing the system over the network.

The "Send NTLM response only" setting is an improvement, but it still leaves password hashes susceptible to being captured by sniffers and cracked off-line.

Disabling network access to the CD and floppy drives is a simple measure to protect against the forgetful administrator who leaves critical media in either drive. Of course, poor physical security easily defeats this protection.

Improvements were made to SMB authentication by adding the option to digitally sign the SMB packets. But leaving the setting at "when possible" still leaves the system open to "man-in-the-middle" and session attacks when digital signatures are not possible.

The discrepancy between the recommended settings for the "Configure Smart Card Removal Behavior" parameter is an area where Microsoft's recommendations may cause more problems than it protects against. By forcing logoff, client sessions may not be properly terminated which could in turn lead to other unintended consequences. Locking the workstation is sufficient for security purposes.

Driver signing is important because drivers are installed in Kernel mode. Consequently, malicious drivers can bypass virtually all controls. While it would be ideal to never allow the installation of unsigned drivers, this is not always possible due to the rapid changes in the technology industry. However, sufficient progress has been made that SANS now recommends that the installation of unsigned drivers no longer be allowed. Similar capabilities are provided for non-driver devices. Microsoft and SANS are in agreement that it is sufficient to issue a warning before allowing such drivers to be installed.

Hisecdc Security Template

Overview

As its name implies, the hisecdc template represents the highest security level template provided by Microsoft. It should be remembered though that this template is primarily intended to secure Windows 2000 network communications. The changes below bear this out.

As before discrepancies are marked in yellow.

Template

Section	Description	Step By Step	Hisecdc Settings
3.1.1	Account Policy		
	Account Lockout Duration	4 Hours	0 Minutes
3.1.2.1	Audit Policy		
	Account Logon Events	Success, Failure	Success, Failure
	Account Management	Success, Failure	Success, Failure
	Logon Events	Success, Failure	Success, Failure
	Object Access	Success, Failure	Success, Failure
	Policy Change	Success, Failure	Success, Failure
	Privilege Use	Success, Failure	Success, Failure
	Process Tracking	Not Specified	No Auditing
	System Events	Success, Failure	Success, Failure
3.1.2.3	Security Options		
3.1.2.3.1	Additional restrictions for anonymous connections	No Access Without Explicit Restrictions	No Access Without Explicit Restrictions
3.1.2.3.9	Clear Virtual Memory Pagefile When System Shuts Down	Enable	Enabled
3.1.2.3.10	Digitally Sign Client	When Possible	Always

Section	Description	Step By Step	Hisecdc Settings
	Communication		
3.1.2.3.11	Digitally Sign Server Communication	When Possible	Always
3.1.2.3.13	Do Not Display Last User Name in Logon Screen	Enable	Enabled
3.1.2.3.14	LAN Manager Authentication Level	Send NTLMv2 response only	Send NTLMv2 response only/Refuse LM and NTLM
3.1.2.3.24	Secure the Netlogon Channel	Require strong (Windows 2000 or later) session key	Require strong (Windows 2000 or later) session key
3.1.2.3.29	Configure Unsigned Non-Driver Installation Behavior	Warn but allow installation	Succeed silently
3.3.1.1	Maximum Log Size	Enough to last between full backups	Security Log Increased to 10MB

Analysis

The hisecdc template takes another step closer to the SANS recommendations. Auditing is brought up to the levels recommended. Anonymous connections are restricted to the greatest extent possible. The pagefile is cleared during shutdown protecting it from being inspected if the system is booted to an alternate OS such as Linux. All client and server communications are always digitally signed. If the site's physical security is compromised, the user that last logged on is not revealed. Authentication is now at the highest level, and lower levels are refused. The Netlogon channel carries the highest level of encryption.

According to Microsoft the predefined templates are additive in nature. That is as each more secure template is imported, it should increase the security stance of the server. However, it can also add errors. For some strange reason the hisecdc template inexplicably **lowers** the Account Lockout Duration from 30 minutes to 0. It also **lowers** the security setting for the "Configure Unsigned Non-Driver Installation Behavior" to succeed silently. These settings are surely a mistake and should not be accepted.

Because the Netlogon channel is secured with the "Require strong (Windows 2000 or later) session key" setting, this security policy can only be used in pure Windows 2000 networks. In heterogeneous networks that include Windows 9x, Windows ME or Windows NT systems, this setting is not appropriate and should be disabled.

Final Analysis Of The Microsoft Security Templates

Overview

After applying the Microsoft predefined security templates, the security stance of the server should be reviewed against the SANS Windows 2000 Step By Step recommendations to determine whether it is correctly configured for production use.

The following table lists all of the SANS recommendations and compares them to the Microsoft settings. Areas still not meeting the SANS recommendations are highlighted in yellow.

Template

Section	Description	Step By Step	Installed Settings
3.1.1	**Account Policy**		
	Enforce Password History	8 – 13 Passwords	24 Password
	Maximum Password Age	45 – 90 Days	42 Days
	Minimum Password Age	1 – 5 Days	2 Days
	Minimum Password Length	8 Characters	8 Characters
	Passwords must meet complexity requirements	Enabled	Enabled
	Store passwords using reversible encryption for all users in the domain	Disabled	Disabled
	Account Lockout Duration	4 Hours	0 Minutes
	Account Lockout Threshold	5 Failed Attempts	5
	Reset Account Lockout Counter After	4 Hours	30 Minutes
3.1.2	**Local Policy**		
3.1.2.1	**Audit Policy**		
	Account Logon Events	Success, Failure	Success, Failure
	Account Management	Success, Failure	Success, Failure
	Logon Events	Success, Failure	Success, Failure
	Object Access	Success, Failure	Success, Failure
	Policy Change	Success, Failure	Success, Failure

Section	Description	Step By Step	Installed Settings
	Privilege Use	Success, Failure	Success, Failure
	Process Tracking	Not Specified	No Auditing
	System Events	Success, Failure	Success, Failure
3.1.2.2	**User Rights**		
	Access this computer from the network	Domain Users	Administrators, IWAM, IUSR, Authenticated Users, Everyone
	Act as part of the operating system	None	None
	Add workstations to domain	Administrators	Authenticated Users
	Backup files and directories		Backup Operators, Administrators, Server Operators
	Bypass traverse checking	Administrators, Server Operators and Backup Operators	Administrators, Authenticated Users, Everyone
	Change the system time	Administrators	Server operators, Administrators
	Create a page file	Domain Administrators	Administrators
	Create a token object	None	None
	Create permanent shared objects		None

Section	Description	Step By Step	Installed Settings
	Debug programs	None	Administrators
	Deny access to this computer from the network	Administrators	None
	Deny logon as a batch job	Not Specified	None
	Deny logon as a service	Not Specified	None
	Deny logon locally	Not Specified	None
	Enable computer and user accounts to be trusted for delegation	Not Specified	Administrators
	Force shutdown from a remote system	Not Specified	Server Operators, Administrators
	Generate security audits	Not Specified	None
	Increase quotas	Not Specified	Administrators
	Increase scheduling	Administrators	Administrators
	Load and unload device drivers	Administrators	Administrators
	Lock pages in memory	None	None
	Logon as a batch job	None	IWAM, IUSR
	Logon as a service	None	None
	Logon locally	Administrators, Server Operators and Backup Operators	Backup Operators, Print Operators, Server Operators, Account Operators,

Section	Description	Step By Step	Installed Settings
			Administrators
	Manage auditing and security logs	Administrators	Administrators
	Modify firmware environment values	Administrators, Server Operators and Backup Operators	Administrators
	Profile single process	Not Specified	Administrators
	Profile system performance	Not Specified	Administrators
	Remove computer from docking station	Not Specified	Administrators
	Replace a process level token	None	None
	Restore files and directories	Backup Operators	Backup Operators, Server Operators, Administrators
	Shutdown the server	Administrators and Server Operators	Backup Operators, Print Operators, Server Operators, Account Operators, Administrators
	Synchronize directory service data	Not Specified	None
	Take ownership of files or other objects	Administrators	Administrators
3.1.2.3	**Security Options**		

Section	Description	Step By Step	Installed Settings
3.1.2.3.1	Additional restrictions for anonymous connections	No Access Without Explicit Restrictions	No Access Without Explicit Restrictions
3.1.2.3.2	Allow Server Operators to Schedule Tasks	Disable	Disabled
3.1.2.3.3	Allow System to be Shut Down Without Having to Log On	Enable only at sites with strong physical security	Disabled
3.1.2.3.4	Allowed to Eject Removable NTFS Media	Not Specified	Administrators
3.1.2.3.5	Amount of Idle Time Required Before Disconnecting Session	15 Minutes	15 Minutes
3.1.2.3.6	Audit the Access of Global System Objects	Undefined or Disabled	Disabled
3.1.2.3.7	Audit Use of Backup and Restore Privilege	Enable	Disabled
3.1.2.3.8	Automatically Log Off Users When Logon Time Expires	Enable	Enabled
3.1.2.3.9	Clear Virtual Memory Pagefile When System Shuts Down	Enable	Enabled
3.1.2.3.10	Digitally Sign Client Communication	When Possible	Always
3.1.2.3.11	Digitally Sign Server Communication	When Possible	Always
3.1.2.3.12	Disable CTRL+ALT+DEL	Disable	Disabled

Section	Description	Step By Step	Installed Settings
	Requirement for Logon		
3.1.2.3.13	Do Not Display Last User Name in Logon Screen	Enable	Enabled
3.1.2.3.14	LAN Manager Authentication Level	Send NTLMv2 response only	Send NTLMv2 response only/refuse LM and NTLM
3.1.2.3.15	Message Text/Title for users attempting to Logon	Provide text after consulting with legal counsel	None
3.1.2.3.16	Number of Previous Logons to Cache	0	10
3.1.2.3.17	Prevent System Maintenance of Computer Account Password	Disable	Disabled
3.1.2.3.18	Prevent Users From Installing Print Drivers	Enable	Enabled
3.1.2.3.19	Prompt User to Change Password Before Expiration	14 Days	14 Days
3.1.2.3.20	Recovery Console: Allow Automatic Administrative Logon	Disable	Disabled
3.1.2.3.21	Recovery Console: Allow Floppy Copy and Access to All Drives and Folders	Disable	Disabled
3.1.2.3.23	Restrict the CD-ROM and Floppy drive access to locally logged on user only	Enable	Enabled

Section	Description	Step By Step	Installed Settings
3.1.2.3.24	Secure the Netlogon Channel	Require strong (Windows 2000 or later) session key	Require strong (Windows 2000 or later) session key
3.1.2.3.25	Send Unencrypted Password to Connect to Third-Party SMB Servers	Disable	Disabled
3.1.2.3.26	Shut Down System Immediately If Unable to Log Security Audits	Enable (with care)	Disabled
3.1.2.3.27	Configure Smart Card Removal Behavior	Lock the workstation	Force Logoff
3.1.2.3.28	Configure Unsigned Driver Installation Behavior	Do not allow installation	Do not allow installation
3.1.2.3.29	Configure Unsigned Non-Driver Installation Behavior	Warn but allow installation	Succeed silently
3.3.1.1	Maximum Log Size	Enough to last between full backups	512 KB
	Retention Period	Days between full backups	7 Days
	Retention Method	By Days	By Days
3.3.2.1	WMI Control	Disable if not needed	Not Defined
3.3.2.3	Indexing Service	Disable if not needed	Not Defined

Analysis

By examining the table above it becomes clear that the Microsoft settings still fall short of SANS recommendations. These shortcomings primarily deal with managing users through account lockout policies and user rights. This is probably due to Microsoft trying to reconcile two conflicting "features" – high security and ease of operation. For instance while it may be much more convenient to be able to manage the server from anywhere on the network, it is more secure to restrict administrative activities to the server console.

Potentially Unnecessary Services

While on the subject of convenience, it should be noted that SANS makes several specific suggestions on services that can be disabled that have not yet been addressed in this paper. The reason for this is that what services need to be running is very dependent on what role the server will be playing in the network. If it is a web server, then the WWW Publishing Service should be running and automatically started at boot time. If it is to be a Kerberos authentication server, this would not be the case.

Microsoft, like every other operating system vendors, tends to choose installation defaults that have more services running than is necessary. This ties back to the above conflict. The user perception is more favorable if the server is ready to perform a task regardless of the security consequences. Since Microsoft wants Windows 2000 perceived as powerful but easy to use, it enables services that may never be required. As an example, does every server need to be configured as a Kerberos Key Distribution Center? Undoubtedly, not. However, by default that server is automatically installed and enabled by the default Windows 2000 Server installation.

But it is possible to disable all the services recommended by SANS except those whose functions are clearly in line with the server's role. Then as testing is done before putting the server into production, any missing services can be re-enabled. As the cliché goes, your mileage may vary.

The following are the services that SANS recommends be disabled if they are not necessary. The list is separated into two categories based on whether the default, installed startup mode is manual or automatic.

Automatically Started Services:

Alerter
Application Management
Computer Browser
Distributed File System
Distributed Link Tracking Client

Distributed Link Tracking Server
DNS Client
Intersite Messaging
Kerberos Key Distribution Center
Messenger
Print Spooler
Server
TCP/IP NetBIOS Helper
Terminal Server
Uninterruptible Power Supply
Workstation

Manually Started Services:

Clipbook
FAX Service
File Replicationi
Internet Connection Sharing
NetMeeting Remote Desktop Sharing
QoS RSVP
Remote Access Auto Connection Manager
Remote Access Connection Manager
Smart Card
Smart Card Helper
Telephony
Telnet
Utility Manager

Conclusions

It is safe to say that implementing the changes to the manually started services probably will not make a difference in the functionality of the server since they are not running anyway. However, the list of automatically started services should be studied carefully to determine if they are required for the role the server is intended to play.

Through the use of SCAT, it is possible to finish the job that Microsoft began. To do so simply take the discrepancies found in the table above, and then change the settings to correspond to the SANS recommendation.

When creating a new file

SANS Windows 2000 Template

Overview

A sample template that implements the SANS Windows 2000 recommendations is provided in Appendix B. Explaining the format of the entries in the template is beyond the scope of this paper. To review the settings it is recommended that the entries be pasted into a file created in %WINDIR%\security\templates. Be sure that its name ends with .inf so that the file is associated with SCAT. Finally, use SCAT to view each value.

Analysis

The template implements as many of the SANS recommendations as SCAT is capable of implementing. With this template the process of securing a new Windows 2000 Server installation is greatly simplified and speeded up. It also reduces the possibility of human error in securing the server. Finally, it ensures a consistent starting point for servers as they are brought on-line in the enterprise.

Conclusions Regarding SCAT And The Pre-Defined Security Templates

The Security Configuration and Analysis Tool in combination with the Microsoft Security Templates substantially improves the security stance of a newly installed server. However, it does contain some inexplicable settings that should not be relied upon. In doing so it points out the dangers of blindly and complacently accepting the findings of a tool without detailed review.

Even without the inexplicable settings, the security templates still do not meet all of the recommendations made by SANS. In general the user rights they permit are too lax, they make no attempt to establish file or registry permissions, and they make no attempt to control unnecessary services. Finally, SCAT itself is incapable of changing registry key values leaving these adjustments to be made manually.

A major shortcoming of SCAT is its lack of a reporting function that clearly lists all the settings of a given template. The next best thing is to print the template file itself since it is just a CSV text file. This does have the benefit that you can copy and paste it or any portion of it into another file that can be then be opened by SCAT.

Security Via Scripting

Overview

Windows 2000 comes with the Windows Script Host Version 2 (WSH2). WSH allows for the direct execution of command scripts written in various scripting tools such as VBScript and Jscript. WSH has an open interface so third party vendors can integrate other scripting languages such as Perl or Tcl. Scripts can be executed directly from the command line, by double-clicking on their icons in Windows Explorer or from HTML pages.

Two versions of WSH are provided. Cscript is used from the command line and provides command line parameters that augment the scripts. Wscript is used from within the Windows environment.

Scripts are similar to Unix shell scripts or DOS bat files. However, due to the extended capabilities of either VBScript or Jscript, WSH greatly expands what can be done. Compared to bat files, WSH scripts have superior branching capabilities and looping capabilities. More importantly, they can take advantage of ActiveX components that expose their properties and methods.

Windows 2000 also comes with Microsoft Script Editor and Microsoft Script Debugger to aid with the development of script routines.

It is beyond the scope of this paper to provide a detailed explanation of either VBScript or Jscript. However, a general explanation will be provided of VBScript so that a demonstration of the value of scripting to the process of securing a server can be presented.

VBScript Semantics

While lacking true object-oriented features such as inheritance, both VBScript and Jscript use an object-oriented like command structure.

An object is a software entity of related properties and methods. For instance a word would be an example of a simple object.

Objects can be part of other objects, or it can be a collection of like objects. For instance, words are grouped into sentences, sentences are grouped into paragraphs, and paragraphs are grouped into documents.

An object has properties. A word in a document has a font, color and size.

An object's properties are manipulated by methods directly associated with the object. For example, a word can have methods to change its font, color or size.

In VBScript objects are referred to in a hierarchy called an object model. In VBScript the object model is represented with the following notation:

```
Object1.Object2.Object3
```

Following the example above:

```
Document.Paragraph.Sentence.Word
```

A property is just an extension of the above format:

```
Document.Paragraph.Sentence.Word.Font
```

Similarly, a method uses the same type of extension of the format:

```
Document.Paragraph.Sentence.Word.ChangeFont
```

Manipulating the value of an object property is accomplished by calling the appropriate method of the property with the new value for the property as an argument to the call. For instance, to display a word in the Tahoma font, the statement might look like:

```
Document.Paragraph.Sentence.Word.ChangeFont(Tahoma)
```

VBScript also has the ability to do conditional execution of statements. In other words it can take different actions based on the situation at the time the action is to be performed. The format for conditional execution is:

```
If true then
        Do this
Else
        Do that
End if
```

VBScript also has the ability to loop or execute the same set of statements repeatedly. A loop is executed until some condition becomes true. The two primary looping mechanisms in VBScript are Do loops and For loops.

The most often used format of the Do loop is the Do Until loop:

```
Do Until true
        Command 1
        Command 2
                .
                .
        Command n
Loop
```

For loops can be of one of two types: For…Next and For Each…Next.

A For…Next loop repeats a set of commands that will be executed a finite number of times. Its format is:

```
For I = Start To End
    Command 1
    Command 2
        .
        .
    Command n
Next
```

A For Each…Next executes a set of commands for each item in a list. Its format is:

```
For Each Item In List
    Command 1
    Command 2
        .
        .
    Command n
Next
```

VBScript also provides two mechanisms, functions and procedures, which are used to define a group of commands that can be used whenever needed. Functions are used when a single value needs to be returned. Procedures are used when it is not necessary to return a value.

The format for Functions is:

```
Function Name(Parameters)
    Command 1
    Command 2
        .
        .
    Command n
End Function
```

The syntax for Procedures is:

```
Sub Name(Parameters)
    Command 1
    Command 2
        .
        .
    Command n
End Sub
```

Registry Overview

The Windows Registry is a database that stores internal configuration data for the local system. The Registry acts as a common repository for programs to store persistent parameters. It is arranged in a hierarchical tree of keys, subkeys, and values. Windows 2000 has the following five root keys or hives.

The HKEY_LOCAL_MACHINE root key contains information about the local computer system, including hardware and operating system data such as bus type, system memory, device drivers, and startup control parameters. It is this root key that is most often used to set and change system parameters.

The HKEY_CLASSES_ROOT contains data that either associates file types with programs or is configuration data for COM objects. It also contains the data stored in HKEY_USERS\<SID>_Classes.

The HKEY_USERS subtree contains all actively loaded user profiles. HKEY_USERS has at least three subkeys. The .DEFAULT subkey stores the profile used when no users are logged onto the computer. At least one subkey exists for the current local user and is named with the user's Security Identifier (SID). This subkey contains the current user's profile. The last subkey contains the current user's Classes. It also uses the SID of the current local user with the _Classes suffix for its name.

The HKEY_CURRENT_CONFIG stores configuration data for the current hardware profile. This root key just stores a pointer to the data stored in HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Hardware Profiles\Current so any changes that need to be made can be made in either location.

Like HKEY_CURRENT_CONFIG, HKEY_CURRENT_USER stores a pointer to the content of HKEY_USERS\<SID of current user> and changes can be made in either location.

The root keys are comprised of keys, subkeys, and value names. An entry is the lowest level item and is where data is actually stored. Entries have a name, data type and value.

Data is stored in the following primary data types:

- REG_SZ – string values
- REG_BINARY – binary values
- REG_DWORD – 32 bit binary data type represented in either decimal or hexadecimal formats.
- REG_MULTI_SZ – multiple string values
- REG_EXPAND_SZ – expandable strings

While certainly not a comprehensive list of the capabilities of VBScript or the Registry, this should provide an understanding sufficient to follow the example that will be presented later.

Sample VBScript to Set Registry Values

Although the Security Configuration and Analysis Tool is capable of implementing many of the SANS recommendations, a significant shortcoming is its inability to set Registry values.

The following is a list of the Registry keys that SANS recommends be adjusted:

- Disable Autorun on CD-Rom Drives
- Enforce Anonymous Named Pipe control
- Restrict Null User access to Shares
- Mitigate the Risk of Syn Flood Attacks
- Disable Router Discovery
- Disable IP Source Routing
- Tune the TCP/IP KeepAlive Timer
- Disable ICMP Redirects
- Disable External Name Release
- Disable DCOM
- Remove the AEDebug Key
- Remove Administrative Shares
- Disable 8.3 Filename Creation

If IIS is installed, SANS makes additional recommendations:

- Enable Logging of SSL Errors and Warnings
- Disable Use Of The Command Shell With #exec
- Remove RDS Functionality
- Enable Directory Annotation

The following is a sample VBScript that makes the recommended changes to the registry. It does not implement the changes recommended for IIS. (Should you choose to try this script, bear in mind it is written by a student attempting to pass SANS certification requirements. You should back up the Registry before running this script and verify carefully that it will operate as intended.)

```
'==========================================================================
'
' NAME: SecureW2KRegistry.vbs
'
' AUTHOR: John M. Millican , New Concept Technologies, Akron, OH
' DATE  : 4/1/2001
'
' COMMENT:      Used to automatically set the Registry values recommended by the
'               SANS Institute in "Securing Windows 2000 Step by Step".
'
'==========================================================================
Dim Hive, key, valname, valx

'   Initialize variables.
Hive = "HKEY_LOCAL_MACHINE\"
```

```
ServicesPath = "System\CurrentControlSet\Services\"
ControlPath = "System\CurrentControlSet\Control\"
CurrentVersionPath = "Software\Microsoft\WindowsNT\CurrentVersion\"
MicrosoftPath = "Software\Microsoft\"
IFName = "{BF45C645-D627-42E9-A104-212D58A42AE2}"

'   Check To See If The Key Exists
Function KeyExists(key)
        Dim key2
        On Error Resume Next
        key2 = Registry.RegRead(key)
        if Err <> 0 Then
                KeyExists = False
        Else
                KeyExists = True
        End If
        On Error GoTo 0
End Function

'   Create the  object that will be associated with the Registry
Dim Registry
Set Registry = WScript.CreateObject("WScript.Shell")

'  Command format to write a value to a Registry key
'  Registry.RegWrite KeyPathName, Value, Type

'  Command format to delete a Registry key value
'  Registry.RegDelete "KeyPathValueName
'  Disable Autorun on CD-Rom Drives
   Registry.RegWrite ServicesPath & "Services\CDRom\Autorun", 0, "REG_DWORD"

'  Enforce Anonymous Named Pipe control
   Registry.RegWrite ServicesPath & "LanManServer\Parameters\NullSessionPipes" 1, "REG_DWORD"

'  Restrict Null User access to Shares
   Registry.RegWrite ServicesPath & "LanManServer\Parameters\NullSessionShares" "", "REG_MULTI_SZ"

'  Mitigate the Risk of Syn Flood Attacks
   Registry.RegWrite ServicesPath & "Tcpip\Parameters\SynAttackProtect", 2, "REG_DWORD"

'  Disable Router Discovery
   Registry.RegWrite ServicesPath & "Tcpip\Parameters\Interfaces\" & IFName, 0, "REG_DWORD"

'  Disable IP Source Routing
   Registry.RegWrite ServicesPath & "Tcpip\Parameters\DisableIPSourceRouting", 1, "REG_DWORD"

'  Tune the TCP/IP KeepAlive Timer
   Registry.RegWrite ServicesPath & "Tcpip\Parameters\KeepAliveTimer", 300000, "REG_DWORD"

'  Disable ICMP Redirects
   Registry.RegWrite ServicesPath & "Tcpip\Parameters\EnableICMPRedirects", 0 "REG_DWORD"

'  Disable External Name Release
   Registry.RegWrite ServicesPath & "Tcpip\Parameters\NoNameReleaseOnDemand", 1, "REG_DWORD"

'  Disable DCOM
   Registry.RegWrite MicrosoftPath & "OLE\EnableDCOM", "N", "REG_SZ"

'  Remove the AEDebug Key
```

```
  If KeyExists("HKLM\Software\Microsoft\WindowsNT\CurrentVersion\AEDebug\Debugger") Then
    Registry.RegDelete "HKLM\Software\Microsoft\WindowsNT\CurrentVersion\AEDebug\Debugger"
  End If

'  Remove Administrative Shares
  If KeyExists("HKLM\System\CurrentControlSet\Services\LanmanServer\Parameters\AutoShareServer") Then
    Registry.RegDelete "HKLM\System\CurrentControlSet\Services\LanmanServer\Parameters\AutoShareServer"
  End If

'  Disable 8.3 Filename Creation
  Registry.RegWrite ControlPath & "Filesystem\NTFSDisable8dot3NameCreation", 1, "REG_DWORD"

'*** End
```

Summary

Given the dramatic increase in features and complexity of Windows 2000, the Security Configuration Tool Set provided with it was a necessity. And while Microsoft provides a good foundation in securing the server, the job is not complete.

That is not a knock on Microsoft. They appear to be at least as intent as any other operating system vendor in providing secure servers. Microsoft definitely has the marketing savvy to know that server security is a selling benefit in the market for which Windows 2000 is targeted.

However, every tool must be viewed as a mechanism used to achieve an objective. It does not free administrators of their responsibility to know and understand the tools available to them. It is also the administrators' responsibility to know how and when to use those tools. Relying on a tool blindly is as dangerous as not using it at all. Tools can give a false sense of security.

This is certainly the case with the Security Configuration Tool Set. It is an excellent tool in the right hands. SCAT provides a very effective means to secure a system. The Security Templates handle many of the issues that must be addressed.

However, SCAT is not capable of making all the adjustments necessary to fully secure a server for use in a production environment. It cannot modify values in the Registry, and its reporting capabilities are limited. The Security Templates do not set every security option to its highest level. In fact they apparently contain errors. The Windows Script Host in conjunction with VBScript or Jscript is a powerful supplement to these tools and to address some of their shortcomings.

In the final analysis it is still the administrator's responsibility to know the tools at their disposal and to make appropriate use of them. A golfer would not use a driver to sink an important putt. Administrators should show the same good judgment.

Appendix A – Acknowledgements and Sources

Shawgo, Jeff editor. Windows 2000 Security Step By Step. A Survival Guide For Windows 2000 Security. SANS Institute. 2001

Born, Gunter. Microsoft Windows Script Host 2.0 Developer's Guide. Microsoft Press. 2000

"MS Security Tool Set". Microsoft TechNet. June 7, 2000
URL: http://www.microsoft.com/technet/win2000/win2ksrv/technote/securcon.asp

Resource Kit Technical Reference To The Registry. Microsoft Corporation. 2000.

Resource Kit Technical Group Policy Reference. Microsoft Corporation. 2000.

Appendix B – Sample SANS Windows 2000 SCAT Template

```
[Unicode]
Unicode=yes
[Version]
signature="$CHICAGO$"
Revision=1
[Profile Description]
Description=Assumes clean-install NTFS file\reg ACLs. Includes SecureDC settings with Windows
2000-only enhancements. Empties Power Users group.
[System Access]
MinimumPasswordAge = 2
MaximumPasswordAge = 42
MinimumPasswordLength = 8
PasswordComplexity = 1
PasswordHistorySize = 24
LockoutBadCount = 5
ResetLockoutCount = 480
LockoutDuration = 480
RequireLogonToChangePassword = 0
ForceLogoffWhenHourExpire = 1
ClearTextPassword = 0
[System Log]
MaximumLogSize = 512
AuditLogRetentionPeriod = 1
RetentionDays = 7
RestrictGuestAccess = 1
[Security Log]
MaximumLogSize = 10240
AuditLogRetentionPeriod = 0
RetentionDays = 7
RestrictGuestAccess = 1
[Application Log]
MaximumLogSize = 512
AuditLogRetentionPeriod = 1
RetentionDays = 7
RestrictGuestAccess = 1
[Event Audit]
AuditSystemEvents = 3
AuditLogonEvents = 3
AuditObjectAccess = 3
AuditPrivilegeUse = 3
AuditPolicyChange = 3
AuditAccountManage = 3
AuditProcessTracking = 0
AuditDSAccess = 3
AuditAccountLogon = 3
[Registry Values]
machine\system\currentcontrolset\services\netlogon\parameters\signsecurechannel=4,1
machine\system\currentcontrolset\services\netlogon\parameters\sealsecurechannel=4,1
```

```
machine\system\currentcontrolset\services\netlogon\parameters\requirestrongkey=4,1
machine\system\currentcontrolset\services\netlogon\parameters\requiresignorseal=4,1
machine\system\currentcontrolset\services\netlogon\parameters\disablepasswordchange=4,0
machine\system\currentcontrolset\services\lanmanworkstation\parameters\requiresecuritysignature=4,1
machine\system\currentcontrolset\services\lanmanworkstation\parameters\enablesecuritysignature=4,1
machine\system\currentcontrolset\services\lanmanworkstation\parameters\enableplaintextpassword=4,0
machine\system\currentcontrolset\services\lanmanserver\parameters\requiresecuritysignature=4,1
machine\system\currentcontrolset\services\lanmanserver\parameters\enablesecuritysignature=4,1
machine\system\currentcontrolset\services\lanmanserver\parameters\enableforcedlogoff=4,1
machine\system\currentcontrolset\services\lanmanserver\parameters\autodisconnect=4,15
machine\system\currentcontrolset\control\session manager\protectionmode=4,1
machine\system\currentcontrolset\control\session manager\memory management\clearpagefileatshutdown=4,1
machine\system\currentcontrolset\control\print\providers\lanman print services\servers\addprinterdrivers=4,1
machine\system\currentcontrolset\control\lsa\submitcontrol=4,0
machine\system\currentcontrolset\control\lsa\restrictanonymous=4,2
machine\system\currentcontrolset\control\lsa\lmcompatibilitylevel=4,5
machine\system\currentcontrolset\control\lsa\fullprivilegeauditing=3,0
machine\system\currentcontrolset\control\lsa\crashonauditfail=4,0
machine\system\currentcontrolset\control\lsa\auditbaseobjects=4,0
machine\software\microsoft\windows\currentversion\policies\system\shutdownwithoutlogon=4,0
machine\software\microsoft\windows\currentversion\policies\system\legalnoticetext=1,WARNING USE OF THIS PRIVATE COMPUTER SYSTEM IS YOUR CONSENT TO BEING MONITORED AND RECORDED. UNAUTHORIZED USE IS PROHIBITED. WE RESERVE THE RIGHT TO SEEK ALL REMEDIES FOR UNAUTHORIZED USE. EVIDENCE OF SUSPECTED ILLEGAL USE MAY BE GIVEN TO LAW ENFORCEMENT.
machine\software\microsoft\windows\currentversion\policies\system\legalnoticecaption=1,Usage Warning
machine\software\microsoft\windows\currentversion\policies\system\dontdisplaylastusername=4,1
machine\software\microsoft\windows\currentversion\policies\system\disablecad=4,0
machine\software\microsoft\windows nt\currentversion\winlogon\scremoveoption=1,1
machine\software\microsoft\windows nt\currentversion\winlogon\passwordexpirywarning=4,14
machine\software\microsoft\windows nt\currentversion\winlogon\cachedlogonscount=1,0
machine\software\microsoft\windows nt\currentversion\winlogon\allocatefloppies=1,1
machine\software\microsoft\windows nt\currentversion\winlogon\allocatedasd=1,0
machine\software\microsoft\windows nt\currentversion\winlogon\allocatecdroms=1,1
machine\software\microsoft\windows nt\currentversion\setup\recoveryconsole\setcommand=4,0
machine\software\microsoft\windows nt\currentversion\setup\recoveryconsole\securitylevel=4,0
machine\software\microsoft\non-driver signing\policy=3,0
machine\software\microsoft\driver signing\policy=3,2
[Privilege Rights]
sebatchlogonright =
sechangenotifyprivilege = *S-1-5-32-551,*S-1-5-32-549,*S-1-5-32-544
secreatepagefileprivilege = *S-1-5-21-1004336348-764733703-854245398-512
sedenynetworklogonright = *S-1-5-32-544
seinteractivelogonright = *S-1-5-32-551,*S-1-5-32-549,*S-1-5-32-544
```

```
semachineaccountprivilege = *S-1-5-32-544
senetworklogonright = *S-1-5-21-1004336348-764733703-854245398-513
serestoreprivilege = *S-1-5-32-551
sesystemtimeprivilege = *S-1-5-32-544
[Registry Keys]
1="machine\hardware", 0, "D:PAR(A;CI;KA;;;BA)(A;CI;KR;;;WD)(A;CI;KA;;;SY)"
2="machine\sam", 0,
"D:PAR(A;CI;KA;;;BA)(A;CI;KR;;;WD)(A;CI;KA;;;SY)S:PAR(AU;OICISAFA;KA;;;WD)"
3="machine\security", 0, "D:PAR(A;CI;KA;;;BA)(A;CI;KA;;;SY)S:PAR(AU;OICISAFA;KA;;;WD)"
4="machine\software", 2, "D:PAR(A;CI;KA;;;BA)(A;CI;KR;;;AU)(A;CI;KA;;;SY)"
5="machine\software\classes", 2, "D:(A;CI;GR;;;WD)"
6="machine\software\microsoft\command processor", 2,
"D:PAR(A;CI;KA;;;BA)(A;CI;KR;;;AU)(A;CI;KA;;;SY)S:PAR(AU;OICISAFA;KA;;;WD)"
7="machine\software\microsoft\cryptography", 2,
"D:P(A;CI;GR;;;AU)(A;CI;GR;;;SO)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI;GA;;;CO)"
8="machine\software\microsoft\driver signing", 2,
"D:P(A;CI;GR;;;AU)(A;CI;GR;;;SO)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI;GA;;;CO)"
9="machine\software\microsoft\enterprisecertificates", 2,
"D:P(A;CI;GR;;;AU)(A;CI;GR;;;SO)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI;GA;;;CO)"
a="machine\software\microsoft\netdde", 2, "D:P(A;CI;GA;;;BA)(A;CI;GA;;;SY)"
b="machine\software\microsoft\non-driver signing", 2,
"D:P(A;CI;GR;;;AU)(A;CI;GR;;;SO)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI;GA;;;CO)"
c="machine\software\microsoft\ntds", 2,
"D:P(A;CI;GR;;;AU)(A;CI;GR;;;SO)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI;GA;;;CO)"
d="machine\software\microsoft\ole", 2,
"D:P(A;CI;GR;;;AU)(A;CI;GR;;;SO)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI;GA;;;CO)"
e="machine\software\microsoft\protected storage system provider", 1, "D:AR"
f="machine\software\microsoft\rpc", 2,
"D:P(A;CI;GR;;;AU)(A;CI;GR;;;SO)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI;GA;;;CO)"
10="machine\software\microsoft\systemcertificates", 2,
"D:P(A;CI;GR;;;AU)(A;CI;GR;;;SO)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI;GA;;;CO)"
11="machine\software\microsoft\windows nt\currentversion", 2, "D:(A;CI;GR;;;WD)"
12="machine\software\microsoft\windows nt\currentversion\accessibility", 2,
"D:P(A;CI;GR;;;AU)(A;CI;GR;;;SO)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI;GA;;;CO)"
13="machine\software\microsoft\windows nt\currentversion\aedebug", 2,
"D:P(A;CI;GR;;;AU)(A;CI;GR;;;SO)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI;GA;;;CO)"
14="machine\software\microsoft\windows nt\currentversion\asrcommands", 2,
"D:P(A;CI;GR;;;AU)(A;CI;GR;;;SO)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI;GA;;;CO)(A;CI;GRGWSD;;;
BO)"
15="machine\software\microsoft\windows nt\currentversion\classes", 2,
"D:P(A;CI;GR;;;AU)(A;CI;GR;;;SO)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI;GA;;;CO)"
16="machine\software\microsoft\windows nt\currentversion\drivers32", 2,
"D:P(A;CI;GR;;;AU)(A;CI;GR;;;SO)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI;GA;;;CO)"
17="machine\software\microsoft\windows nt\currentversion\efs", 2,
"D:P(A;CI;GR;;;AU)(A;CI;GR;;;SO)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI;GA;;;CO)"
18="machine\software\microsoft\windows nt\currentversion\font drivers", 2,
"D:P(A;CI;GR;;;AU)(A;CI;GR;;;SO)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI;GA;;;CO)"
19="machine\software\microsoft\windows nt\currentversion\fontmapper", 2,
"D:P(A;CI;GR;;;AU)(A;CI;GR;;;SO)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI;GA;;;CO)"
1a="machine\software\microsoft\windows nt\currentversion\image file execution options", 2,
"D:P(A;CI;GR;;;AU)(A;CI;GR;;;SO)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI;GA;;;CO)"
1b="machine\software\microsoft\windows nt\currentversion\inifilemapping", 2,
"D:P(A;CI;GR;;;AU)(A;CI;GR;;;SO)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI;GA;;;CO)"
```

```
1c="machine\software\microsoft\windows nt\currentversion\perflib", 2,
"D:P(A;CI;GR;;;AU)(A;CI;GR;;;SO)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI;GA;;;CO)"
1d="machine\software\microsoft\windows nt\currentversion\perflib\009", 1, "D:AR"
1e="machine\software\microsoft\windows nt\currentversion\profilelist", 1, "D:AR"
1f="machine\software\microsoft\windows nt\currentversion\secedit", 2,
"D:AR(A;CI;KA;;;BA)(A;CI;KR;;;AU)(A;CIIO;KA;;;CO)(A;CI;KR;;;SO)(A;CI;KA;;;SY)S:PAR(AU;OICI
SAFA;KA;;;WD)"
20="machine\software\microsoft\windows nt\currentversion\svchost", 2,
"D:P(A;CI;GR;;;AU)(A;CI;GR;;;SO)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI;GA;;;CO)"
21="machine\software\microsoft\windows nt\currentversion\time zones", 2,
"D:P(A;CI;GR;;;AU)(A;CI;GR;;;SO)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI;GA;;;CO)"
22="machine\software\microsoft\windows nt\currentversion\windows", 2,
"D:P(A;CI;GR;;;AU)(A;CI;GR;;;SO)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI;GA;;;CO)"
23="machine\software\microsoft\windows\currentversion\explorer\user shell folders", 2,
"D:P(A;CI;GR;;;AU)(A;CI;GR;;;SO)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI;GA;;;CO)"
24="machine\software\microsoft\windows\currentversion\group policy", 1, "D:AR"
25="machine\software\microsoft\windows\currentversion\installer", 1, "D:AR"
26="machine\software\microsoft\windows\currentversion\policies", 1, "D:AR"
27="machine\software\microsoft\windows\currentversion\run", 2,
"D:P(A;CI;GR;;;AU)(A;CI;GR;;;SO)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI;GA;;;CO)"
28="machine\software\microsoft\windows\currentversion\runonce", 2,
"D:AR(A;CI;KA;;;BA)(A;CI;KR;;;AU)(A;CIIO;KA;;;CO)(A;CI;KR;;;SO)(A;CI;KA;;;SY)S:PAR(AU;OICI
SAFA;KA;;;WD)"
29="machine\software\microsoft\windows\currentversion\runonceex", 2,
"D:P(A;CI;GR;;;AU)(A;CI;GR;;;SO)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI;GA;;;CO)"
2a="machine\software\microsoft\windows\currentversion\uninstall", 2,
"D:P(A;CI;GR;;;AU)(A;CI;GR;;;SO)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI;GA;;;CO)"
2b="machine\software\policies", 2,
"D:P(A;CI;GR;;;AU)(A;CI;GR;;;SO)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI;GA;;;CO)"
2c="machine\system", 2,
"D:P(A;CI;GR;;;AU)(A;CI;GR;;;SO)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI;GA;;;CO)"
2d="machine\system\clone", 1, "D:AR"
2e="machine\system\controlset001", 1, "D:AR"
2f="machine\system\controlset002", 1, "D:AR"
30="machine\system\controlset003", 1, "D:AR"
31="machine\system\controlset004", 1, "D:AR"
32="machine\system\controlset005", 1, "D:AR"
33="machine\system\controlset006", 1, "D:AR"
34="machine\system\controlset007", 1, "D:AR"
35="machine\system\controlset008", 1, "D:AR"
36="machine\system\controlset009", 1, "D:AR"
37="machine\system\controlset010", 1, "D:AR"
38="machine\system\currentcontrolset\control", 2,
"D:P(A;CI;GR;;;AU)(A;CI;GRGWSD;;;SO)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI;GA;;;CO)"
39="machine\system\currentcontrolset\control\class", 1, "D:AR"
3a="machine\system\currentcontrolset\control\computername", 2, "D:(A;CI;GR;;;WD)"
3b="machine\system\currentcontrolset\control\contentindex", 2, "D:(A;CI;GR;;;WD)"
3c="machine\system\currentcontrolset\control\graphicsdrivers", 2,
"D:P(A;CI;GR;;;AU)(A;CI;GR;;;SO)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI;GA;;;CO)"
3d="machine\system\currentcontrolset\control\keyboard layout", 2, "D:(A;CI;GR;;;WD)"
3e="machine\system\currentcontrolset\control\keyboard layouts", 2, "D:(A;CI;GR;;;WD)"
3f="machine\system\currentcontrolset\control\lsa", 2,
"D:P(A;CI;GR;;;AU)(A;CI;GR;;;SO)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI;GA;;;CO)"
```

```
40="machine\system\currentcontrolset\control\print\printers", 2, "D:(A;CI;GR;;;WD)"
41="machine\system\currentcontrolset\control\prioritycontrol", 2,
"D:P(A;CI;GR;;;AU)(A;CI;GR;;;SO)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI;GA;;;CO)"
42="machine\system\currentcontrolset\control\productoptions", 2, "D:(A;CI;GR;;;WD)"
43="machine\system\currentcontrolset\control\securepipeservers\winreg", 2,
"D:P(A;CI;GA;;;BA)(A;CI;GR;;;BO)"
44="machine\system\currentcontrolset\control\wmi\security", 2,
"D:P(A;CI;GR;;;BA)(A;CI;GA;;;SY)(A;CI;GA;;;CO)"
45="machine\system\currentcontrolset\enum", 1, "D:AR"
46="machine\system\currentcontrolset\hardware profiles", 1, "D:AR"
47="machine\system\currentcontrolset\services", 2,
"D:P(A;CI;GR;;;AU)(A;CI;GRGWSD;;;SO)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI;GA;;;CO)"
48="machine\system\currentcontrolset\services\eventlog", 2,
"D:P(A;CI;GR;;;AU)(A;CI;GR;;;SO)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI;GA;;;CO)"
49="machine\system\currentcontrolset\services\kdc", 2,
"D:P(A;CI;GR;;;AU)(A;CI;GR;;;SO)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI;GA;;;CO)"
4a="machine\system\currentcontrolset\services\ntds", 2,
"D:P(A;CI;GR;;;AU)(A;CI;GR;;;SO)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI;GA;;;CO)"
4b="machine\system\currentcontrolset\services\ntfrs", 2,
"D:P(A;CI;GR;;;AU)(A;CI;GR;;;SO)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI;GA;;;CO)"
4c="machine\system\currentcontrolset\services\tcpip", 2, "D:(A;CI;GR;;;WD)"
4d="machine\system\currentcontrolset\services\wintrust", 2,
"D:P(A;CI;GR;;;AU)(A;CI;GR;;;SO)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI;GA;;;CO)"
4e="users\.default", 2,
"D:P(A;CI;GR;;;AU)(A;CI;GR;;;SO)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI;GA;;;CO)"
4f="users\.default\software\microsoft\netdde", 2, "D:P(A;CI;GA;;;BA)(A;CI;GA;;;SY)"
50="users\.default\software\microsoft\protected storage system provider", 1, "D:AR"
[File Security]
1="c:\\autoexec.bat", 0, "D:AR(A;OICI;FA;;;BA)(A;OICI;0x1200a9;;;AU)(A;OICI;FA;;;SY)"
2="c:\\boot.ini", 0, "D:AR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
3="c:\\config.sys", 0, "D:AR(A;OICI;FA;;;BA)(A;OICI;0x1200a9;;;AU)(A;OICI;FA;;;SY)"
4="c:\\ntdetect.com", 0, "D:AR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
5="c:\\ntldr", 0, "D:AR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
6="c:\autoexec.bat", 2, "D:P(A;;GRGX;;;AU)(A;;GRGWGXSD;;;SO)(A;;GA;;;BA)(A;;GA;;;SY)"
7="c:\boot.ini", 2, "D:P(A;;GRGWGXSD;;;SO)(A;;GA;;;BA)(A;;GA;;;SY)"
8="c:\config.sys", 2, "D:P(A;;GRGX;;;AU)(A;;GRGWGXSD;;;SO)(A;;GA;;;BA)(A;;GA;;;SY)"
9="c:\documents and settings\all users", 0,
"D:PAR(A;OICI;FA;;;BA)(A;CI;0x1200a9;;;AU)(A;OICI;FR;;;AU)(A;OICI;FA;;;SY)S:PAR(AU;OICIS
AFA;FA;;;BA)(AU;OICISAFA;FA;;;SY)"
a="c:\documents and settings\all users\application data", 0,
"D:PAR(A;OICI;FA;;;BA)(A;CI;0x1200a9;;;AU)(A;OICI;FR;;;AU)(A;OICI;FA;;;SY)"
b="c:\documents and settings\all users\documents", 0,
"D:PAR(A;OICI;FA;;;BA)(A;OICI;CCDCLCDTSD;;;AU)(A;OICI;FA;;;SY)"
c="c:\ntbootdd.sys", 2, "D:P(A;;GRGWGXSD;;;SO)(A;;GA;;;BA)(A;;GA;;;SY)"
d="c:\ntdetect.com", 2, "D:P(A;;GRGWGXSD;;;SO)(A;;GA;;;BA)(A;;GA;;;SY)"
e="c:\ntldr", 2, "D:P(A;;GRGWGXSD;;;SO)(A;;GA;;;BA)(A;;GA;;;SY)"
f="c:\program files", 2, "D:PAR(A;OICI;FA;;;BA)(A;OICI;0x1200a9;;;AU)(A;OICI;FA;;;SY)"
10="c:\winnt", 2, "D:PAR(A;OICI;FA;;;BA)(A;OICI;0x1200a9;;;AU)(A;OICI;FA;;;SY)"
11="c:\winnt\config", 0,
"D:PAR(A;OICI;FA;;;BA)(A;CI;0x1200a9;;;AU)(A;OICI;FR;;;AU)(A;OICI;FA;;;SY)"
12="c:\winnt\debug\usermode", 2,
"D:PAR(A;;0x00100023;;;AU)(A;OIIO;0x00100006;;;AU)(A;CIOI;GRGWGXSD;;;SO)(A;CIOI;GA;;;
BA)(A;CIOI;GA;;;SY)"
```

```
13="c:\winnt\explorer.exe", 2, "D:(A;;GRGX;;;WD)"
14="c:\winnt\installer", 1, "D:AR"
15="c:\winnt\profiles", 1, "D:AR"
16="c:\winnt\regedit.exe", 0,
"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)S:PAR(AU;OICINPSAFA;FA;;;BA)(AU;OICISAFA;FA;;;SY)
"
17="c:\winnt\repair", 2, "D:PAR(A;OICI;FA;;;BA)"
18="c:\winnt\security", 2,
"D:P(A;CIOI;GRGX;;;AU)(A;CIOI;GRGX;;;SO)(A;CIOI;GA;;;BA)(A;CIOI;GA;;;SY)"
19="c:\winnt\system32", 2,
"D:P(A;CIOI;GRGX;;;AU)(A;CIOI;GRGWGXSD;;;SO)(A;CIOI;GA;;;BA)(A;CIOI;GA;;;SY)(A;CIOI;GA
;;;CO)(A;OINP;GRGX;;;WD)"
1a="c:\winnt\system32\autoexec.nt", 2,
"D:P(A;;GRGX;;;AU)(A;;GRGWGXSD;;;SO)(A;;GA;;;BA)(A;;GA;;;SY)"
1b="c:\winnt\system32\cacls.exe", 0,
"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)S:AR(AU;OICISAFA;FA;;;BA)(AU;OICISAFA;FA;;;SY)"
1c="c:\winnt\system32\catroot", 0,
"D:PAR(A;OICI;FA;;;BA)(A;OICI;0x1200a9;;;AU)(A;OICI;FA;;;SY)"
1d="c:\winnt\system32\cmos.ram", 2,
"D:P(A;;GRGX;;;AU)(A;;GRGWGXSD;;;SO)(A;;GA;;;BA)(A;;GA;;;SY)"
1e="c:\winnt\system32\config", 2,
"D:P(A;CI;GRGX;;;AU)(A;CI;GRGX;;;SO)(A;CIOI;GA;;;BA)(A;CIOI;GA;;;SY)(A;CIOI;GA;;;CO)"
1f="c:\winnt\system32\config.nt", 2,
"D:P(A;;GRGX;;;AU)(A;;GRGWGXSD;;;SO)(A;;GA;;;BA)(A;;GA;;;SY)"
20="c:\winnt\system32\cscript.exe", 0,
"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)S:AR(AU;OICISAFA;FA;;;BA)(AU;OICISAFA;FA;;;AU)(AU;
OICISAFA;FA;;;SY)"
21="c:\winnt\system32\dcomcnfg.exe", 0,
"D:AR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)S:AR(AU;OICISAFA;FA;;;BA)(AU;OICISAFA;FA;;;SY)"
22="c:\winnt\system32\dhcp", 2,
"D:P(A;CIOI;GRGX;;;AU)(A;CIOI;GRGX;;;SO)(A;CIOI;GA;;;BA)(A;CIOI;GA;;;SY)(A;CIOI;GA;;;CO)
"
23="c:\winnt\system32\dllcache", 2, "D:P(A;CIOI;GA;;;BA)(A;CIOI;GA;;;SY)"
24="c:\winnt\system32\grouppolicy", 2,
"D:P(A;CIOI;GRGX;;;AU)(A;CIOI;GRGX;;;SO)(A;CIOI;GA;;;BA)(A;CIOI;GA;;;SY)(A;CIOI;GA;;;CO)
"
25="c:\winnt\system32\hpmon.dll", 2, "D:(A;;GRGWGXSD;;;PO)"
26="c:\winnt\system32\hpmon.hlp", 2, "D:(A;;GRGWGXSD;;;PO)"
27="c:\winnt\system32\ias", 2,
"D:P(A;CIOI;GRGWGXSD;;;SO)(A;CIOI;GA;;;BA)(A;CIOI;GA;;;SY)(A;CIOI;GA;;;CO)"
28="c:\winnt\system32\inetsrv\metaback", 0, "D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
29="c:\winnt\system32\inetsrv\metabase.bin", 0, "D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
2a="c:\winnt\system32\midimap.cfg", 2,
"D:P(A;;GRGX;;;AU)(A;;GRGWGXSD;;;SO)(A;;GA;;;BA)(A;;GA;;;SY)"
2b="c:\winnt\system32\net.exe", 0,
"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)S:PAR(AU;OICISAFA;FA;;;BA)(AU;OICISAFA;FA;;;SY)"
2c="c:\winnt\system32\net1.exe", 0,
"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)S:PAR(AU;OICISAFA;FA;;;BA)(AU;OICISAFA;FA;;;SY)"
2d="c:\winnt\system32\ntmsdata", 1, "D:AR"
2e="c:\winnt\system32\rcp.exe", 0,
"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)S:PAR(AU;OICISAFA;FA;;;BA)(AU;OICISAFA;FA;;;SY)"
2f="c:\winnt\system32\regedt32.exe", 0,
"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)S:PAR(AU;OICISAFA;FA;;;BA)(AU;OICISAFA;FA;;;SY)"
```

```
30="c:\winnt\system32\rexec.exe", 0,
"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)S:PAR(AU;OICISAFA;FA;;;BA)(AU;OICISAFA;FA;;;SY)"
31="c:\winnt\system32\rsh.exe", 0,
"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)S:PAR(AU;OICISAFA;FA;;;BA)(AU;OICISAFA;FA;;;SY)"
32="c:\winnt\system32\spool", 2, "D:(A;CIOI;GA;;;PO)"
33="c:\winnt\system32\telnet.exe", 0,
"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)S:PAR(AU;OICISAFA;FA;;;BA)(AU;OICISAFA;FA;;;SY)"
34="c:\winnt\system32\tftp.exe", 0,
"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)S:PAR(AU;OICISAFA;FA;;;BA)(AU;OICISAFA;FA;;;SY)"
35="c:\winnt\system32\wscript.exe", 0,
"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)S:PAR(AU;OICISAFA;FA;;;BA)(AU;OICISAFA;FA;;;SY)"
36="c:\winnt\sysvol", 2,
"D:P(A;CIOI;GRGX;;;AU)(A;CIOI;GRGX;;;SO)(A;CIOI;GA;;;BA)(A;CIOI;GA;;;SY)(A;CIOI;GA;;;CO)
"
37="c:\winnt\sysvol\domain\policies", 2,
"D:P(A;CIOI;GRGX;;;AU)(A;CIOI;GRGX;;;SO)(A;CIOI;GA;;;BA)(A;CIOI;GA;;;SY)(A;CIOI;GA;;;CO)
(A;CIOI;GRGWGXSD;;;PA)"
38="c:\winnt\tasks", 1, "D:AR"
39="c:\winnt\temp", 2, "D:PAR(A;OICI;FA;;;BA)(A;CI;0x100026;;;AU)(A;OICI;FA;;;SY)"
3a="c:\winnt\twain_32", 0, "D:AR(A;OICI;FA;;;BA)(A;OICI;0x1200a9;;;AU)(A;OICI;FA;;;SY)"
[Service General Setting]
1="alerter", 4,
"D:(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPLOCRRC;;;PU)(A;;CCDCLCSWRPWPDTLOCRSDRCW
DWO;;;BA)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SO)(A;;CCLCSWRPWPDTLOCRRC;;;SY)S:(
AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
2="appmgmt", 4,
"D:(A;OICI;CCLCSWLORC;;;WD)(A;OICI;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;OICI;CCL
CSWLORC;;;PU)(A;OICI;CCLCSWRPLO;;;IU)(A;OICI;CCLCSWRPLO;;;BU)S:(AU;FA;CCDCLCSWRP
WPDTLOCRSDRCWDWO;;;WD)"
3="winmgmt", 4,
"D:(A;;CCLCSWRPWPDTLOCRRC;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCS
WLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWD
WO;;;WD)"
4="wmi", 4,
"D:(A;OICI;CCLCSWLORC;;;WD)(A;OICI;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;OICI;CC
DCLCSWLORC;;;PU)(A;OICI;CCLCSWRPLO;;;IU)(A;OICI;CCLCSWRPLO;;;BU)S:(AU;FA;CCDCLCS
WRPWPDTLOCRSDRCWDWO;;;WD)"
```

Last Updated: July 25th, 2017

Upcoming Training

SANS Virginia Beach 2017	**Virginia Beach, VA**	**Aug 21, 2017 - Sep 01, 2017**	**Live Event**
SANS Network Security 2017	**Las Vegas, NV**	**Sep 10, 2017 - Sep 17, 2017**	**Live Event**
SANS vLive - SEC505: Securing Windows and PowerShell Automation	**SEC505 - 201709,**	**Sep 18, 2017 - Nov 13, 2017**	**vLive**
Secure DevOps Summit & Training	**Denver, CO**	**Oct 10, 2017 - Oct 17, 2017**	**Live Event**
SANS San Francisco Winter 2017	**San Francisco, CA**	**Nov 27, 2017 - Dec 02, 2017**	**Live Event**
San Francisco Winter 2017 - SEC505: Securing Windows and PowerShell Automation	**San Francisco, CA**	**Nov 27, 2017 - Dec 02, 2017**	**vLive**
SANS Cyber Defense Initiative 2017	**Washington, DC**	**Dec 12, 2017 - Dec 19, 2017**	**Live Event**
SANS Southern California- Anaheim 2018	**Anaheim, CA**	**Feb 12, 2018 - Feb 17, 2018**	**Live Event**
SANS OnDemand	**Online**	**Anytime**	**Self Paced**
SANS SelfStudy	**Books & MP3s Only**	**Anytime**	**Self Paced**