Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

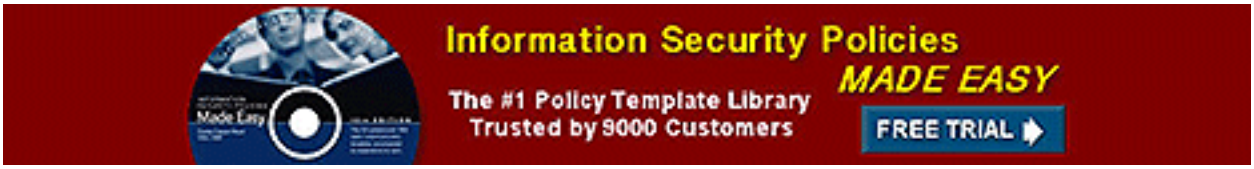
This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Implementing Defense In-Depth at the Department Level

This case study describes the procedures used to improve computer security within my department by following the principles of defense in-depth. It presents a step-by-step approach for improving security by defining risks, assessing vulnerabilities, and implementing measures to reduce the likelihood that those vulnerabilities may be exploited. Finally, the study describes what effect the measures had on overall system security once they were in place. A limited risk assessment was performed to define the department's t...

Copyright SANS Institute
Author Retains Full Rights

AD



Implementing Defense In-Depth at the Department Level

Sean Fahey
GSEC Practical
Version1.4b, Option 2
Submitted February 22, 2004

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Abstract

This case study describes the procedures used to improve computer security within my department by following the principles of defense in-depth. It presents a step-by-step approach for improving security by defining risks, assessing vulnerabilities, and implementing measures to reduce the likelihood that those vulnerabilities may be exploited. Finally, the study describes what effect the measures had on overall system security once they were in place.

A limited risk assessment was performed which defined the department's threats and evaluated them against the vulnerabilities described in the SANS Top 20 List.[1] The assessment was used to identify three areas of security which warranted closer examination. These areas included password management, Windows workstation security (hardening), and Windows patch management. Password management issues were addressed by forcing strong passwords at the workstation level using Novell's single sign-on technology. Windows security was addressed using custom security templates and the Microsoft Security Configuration and Analysis tool. Patch management was addressed using the Windows Automatic Updates feature and verified using Microsoft's Qfecheck utility. Finally, methods including password auditing, port scanning, and patch auditing were used to monitor the impact of the new security measures.

Before

Setting the Scene

This case study took place at my place of employment in a small department composed of three offices each separated by hundreds miles. Each office had its own Novell server running plain vanilla installations of NetWare 5.1 with TCP/IP and IPX. Workstations were Win2K Pro (sp2 or sp4) running the Novell Client for Microsoft (i.e. NetWare Client) over TCP/IP. Neither the Client for Microsoft Networks nor file and print sharing were installed on the workstation and NetBIOS was disabled in the WINS configuration. Symantec AntiVirus was installed on servers and workstations with automated signature updates being pushed out through the servers. The offices were connected to the enterprise WAN over 56K or 128K frame relay circuits. The enterprise IT policy structure was such that each department was fairly autonomous in it's choice of office automation with the exception of major systems such as network operating

[1] SANS top 20.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

system (NetWare), e-mail package (cc:Mail), and the word processing suit (WordPerfect Office). The WAN was protected at its Internet gateways by stateful firewalls and IDS systems yet network traffic within the network perimeter was mostly unmonitored.

Each department within the enterprise was staffed by a single computer systems specialist, sometimes with an assistant, who was responsible for all facets of office automation including computer security. It was the responsibility of each specialist to assure that their systems were as secure as possible to avoid jeopardizing their own operation as well as those of the other departments. If a single workstation were to be compromised within any department it would have been a trivial task for a skilled intruder to map out the entire network looking for targets of opportunity in other departments.

Department procedures and internal controls already dealt specifically with operations security, physical security, contingency and disaster recovery, backup and storage procedures, password policies, and many other policies designed to strengthen computer security. In addition, these procedures were regularly audited by personnel from outside the department. One area that was not specifically addressed in the department's policies was a systematic procedure designed to protect against electronic attacks from hackers. This was due in part to the false sense of security which comes from being behind a firewall and partly from a lack of experience in the information security field . After taking the SANS GSEC course, I learned that by taking a systematic approach to addressing risk through defense in-depth it was possible to achieve efficient and cost effective gains toward improved security. Under these circumstances I decided to perform a limited risk assessment and evaluate the security measures that could mitigate threats from network attacks and malicious code.

Initial Threat Assessment

> *"Although all elements of the risk management cycle are important, risk assessments provide the foundation for other elements of the cycle. In particular, risk assessments provide a basis for establishing appropriate policies and selecting cost-effective techniques to implement these policies."*[2]

The risk assessment phase began by meeting with management and computer specialists from other departments to try and define possible threats from attackers or malicious code. By defining threats we were essentially asking "What assets do we have to protect?" and "What bad things can happen to those assets?" As a result of those meetings I was able to compile the list of threats that are presented in Table 1.

[2] GAO, p. 5.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

The following discussion can be used to define the threats listed in this table. "Electronic assets" were defined as documents, databases, e-mail communications, and other work product stored on the network. Essentially, these were the assets which we had to protect. "Destruction of assets" would entail an unrecoverable erasure or corruption such that the assets would have had to be restored from the backup system. Any files created since the previous night's backup would have been permanently lost had this happened. "Modification of assets" would have occurred if an attacker were to gain access to an asset and modify all or parts of the content. "Theft of assets" would have occurred if an attacker had gained access to the network and copied files offsite.

Table 1
Threat Assessment

Threat	C.I.A. Type[3]	Severity	Likelihood	Level of Concern
Destruction of electronic assets[4]	availability integrity	medium	medium	medium
Modification of electronic assets	integrity	medium	low	low
Theft of electronic assets	confidentiality	medium	low	low
System downtime	availability	medium	high	medium
Systems used as launching pads	confidentiality integrity availability	high	high	high

Another important asset to protect was our reputation. Reliability, confidentiality, and the obligation to take due diligence in performing our duties were key assets that we could not allow to be compromised. Theft of our work product, were it to become public, would have certainly damaged our reputation. "System downtime" would have

[3] C.I.A. refers to confidentiality, integrity, and availability as principles that can be threatened.

[4] Electronic assets are defined as documents, databases, e-mail communications, and other work product stored on the network.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

affected our reliability if we could not perform our duties in a timely fashion. "Systems used as launching pads" referred to the possibility that a workstation or server could have been broken into and used as a launching pad for an attack on other systems and possibly other departments. This could have lead to a very bad situation, both in practical and political terms, possibly resulting in a reduction in funding, network access, and service availability.

Also presented in Table 1 are factors that help evaluate the level of concern associated with each threat. The principles of C.I.A. help define which of the cornerstones of information security are at risk and provide a clearer picture of the type of risk associated with each threat.[5] Severity is classified as high, medium, and low and measures the impact that a threat would have on the department. These can also be thought of as limited, serious, and severe or catastrophic respectively.[6] Likelihood is the probability that a threat could really happen. This can be thought of as a combination of opportunity and motivation. In other words, are there means to carry out the threat and would anyone really care to go to the trouble.

The approach taken here to evaluating threat is known as a qualitative approach since it does not fix a monetary value to the cost of risk. This approach will be taken throughout the risk assessment due to the difficulty of assigning monetary value to assets such as "reliability" and "confidence". This approach is inherently subjective in nature and relies on expertise, experience, and judgment rather than quantified measures of loss.[7] As such, the values assigned for C.I.A., severity, and likelihood in Table 1 are the result of the subjective judgment of myself and department managers. The rational for assigning a specific value to each threat will not be discussed in this paper due to issues of confidentiality. While this method does seem to introduce a high degree of uncertainty "it is important that organizations identify and employ methods that efficiently achieve the benefits of risk assessment while avoiding costly attempts to develop seemingly precise results that are of questionable reliability."[8]

The final column of Table 1 provides a qualitative measure of the level of concern that each of the threats merits. This column is derived by weighing the severity of a threat against the likelihood and number of C.I.A. principles at risk. Additional weight should be given to the severity measure when calculating the final column since a threat that has a low level of severity can in no way be anything more than a minor

---

[5] NIST, p 4. Provides the FISMA and FIPS 199 definitions of C.I.A. as well as a helpful definition of Impact (severity) levels.

[6] NIST, p5.

[7] GAO, pp. 6-7. Provides a good discussion of risk assessment as it applies to information security.

[8] GAO, p. 8.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

concern. Again, while subjective in nature, the resulting level of concern gives a good basis for prioritizing our threats.

During

Vulnerability assessment

Before assessing the risk associated with each threat it is necessary to identify the vulnerabilities that exist to exploit them. Given the classical definition that Risk = Threat X Vulnerability, threat is a function of risk only if vulnerabilities exist to exploiting the threat. Unfortunately, in today's internetworked environment, keeping track of vulnerabilities has become a full-time job for many system administrators. It is often difficult to decide where to start when faced with a growing list of newly discovered vulnerabilities every morning. When faced with such an enormous variety of avenues waiting to be exploited its easy to get lost in the mire. To address this problem a "best practice" approach was used to identify the most important vulnerabilities to assess.

The SANS Top 20 list of Internet Security Vulnerabilities is a "consensus list of vulnerabilities that require immediate remediation."[9] As stated in the SANS list:

> "The vast majority of worms and other successful cyber attacks are made possible by vulnerabilities in a small number of common operating system services. Attackers are opportunistic."[10]

Using the list as a best practices guide to help define the most likely and exploitable vulnerabilities provides a useful foundation for this stage of the analysis. The SANS list provides a step-by-step guide to protecting vulnerable systems from 20 of the most commonly exploited security holes. It is divided into two sections listing 10 windows and 10 Unix/Linux vulnerabilities. Since our network does not include the Unix platform, we will only deal with the Windows vulnerabilities. The SANS top 10 windows vulnerabilities as of this writing are presented in Table 2.

One group of vulnerabilities not included in the SANS Top 20 are those associated with the Novell NetWare servers. This does not mean that NetWare is free from security holes, but only that those holes are not as commonly targeted as those of other operating systems. Several fine resources dealing with NetWare vulnerabilities can be found in the SANS Reading Room,[11] at the BindView Corporation website,[12] or

---

[9] SANS.

[10] SANS.

[11] SANS RR for NetWare specific topics.

[12] Simple Nomad.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

listed on Novell's security alert site.[13] Although these and many other publications demonstrate the need for NetWare vulnerability assessments it was felt that limiting the scope of this assessment to the SANS Top 20 list would help focus our efforts on the vulnerabilities most likely to be exploited.[14] Nevertheless, an analysis of NetWare issues is something that should be performed in our continuing defense in-depth efforts.

Table 2
Vulnerability Analysis

		Mitigated by:		
SANS Top 10 Vulnerabilities (Windows)	**Are we vulnerable?**	**Single Sign-on**	**Security Templates**	**Windows Auto-Update**
Internet Information Services (IIS)	No			
Microsoft SQL Server (MSSQL)	No			
Windows Authentication	Yes	Yes	Yes	Yes
Internet Explorer (IE)	Yes	No	Possibly	Yes
Windows Remote Access Services	Yes	No	Yes	Yes
Microsoft Data Access Components	Yes	No	Possibly	Yes
Windows Scripting Host (WSH)	Yes	No	Yes	Yes
Microsoft Outlook and Outlook Express	No			
Windows Peer to Peer File Sharing (P2P)	No			
Simple Network Management Protocol	No			

Using this list of vulnerabilities we can begin to determine which ones actually pose a threat. Since neither IIS nor MSSQL servers were installed in any of our offices we can safely cross them off the list. Outlook, Outlook Express, and Peer to Peer applications were also not installed on original configurations and since user accounts were part of the standard Windows 2000 "Users" group they were blocked from installing software. Similarly, account restrictions should block all users from installing Peer to Peer software. SNMP was not enabled on any workstation by default and

[13] Novell.

[14] GAO, p. 14. This report argues that a common "best practice" for risk assessments is to limit the scope of the assessment to narrowly defined segments of the system.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

regular NMAP scanning has shown no evidence of either SNMP or Peer to Peer software anywhere on the network. As an added precaution I regularly scan the network using NMAP to verify that none of these packages are running on the network. Since these vulnerabilities do not exist or have already been mitigated they do not require any further action as shown in Table 2. The five remaining vulnerabilities are seen as possible avenues of exploitation and require remediation. Below is a brief explanation of why each posed a threat to the department.

Windows Authentication **-** The four most common password vulnerabilities as defined in the Top 20 list are:

- User accounts have weak or nonexistent passwords.
- Regardless of the strength of their password, users fail to protect it.
- The operating system or additional software creates administrative accounts with weak or nonexistent passwords.
- Password hashing algorithms are known and often hashes are stored such that they are visible by anyone.

The presence of accounts with nonexistent or publicly known passwords are regularly audited as are the services and administrative accounts which create them. In addition, users have been trained to protect their passwords and seem to be very diligent in doing so. While continued attention to these vulnerabilities was warranted, it was not felt that they were areas that required additional remediation.

After review, it was discovered that weak passwords and LM password hashes appeared to be problematic. Prior to this assessment, our typical authentication scenario was to log into the network with the NDS password using the Novell client and let the client automatically change the Windows password so that the two are synchronized. Although Windows 2000 provides powerful tools for enforcing password policy they are much more difficult to implement when logging in with the Novell Client for Windows. In this scenario the Windows password policy rules had to be relaxed to match the much weaker policies incorporated into our version of NetWare (5.1 sp6 ds7.55). Had we not relaxed the Windows rules, NDS would have accepted a password that Windows would have rejected leading to multiple login prompts, user confusion, mismatched passwords, and general mayhem.

In addition, our password policy required a minimum length of only 8 characters and did not specify a requirement for mixed case or special characters. This coupled with the fact that our version of NetWare only enforced the most basic password restrictions it was likely that easily cracked passwords were not only being used in NDS

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

but also being passed down to the Windows SAM database through synchronization.[15] In addition, LM authentication was not disabled on the workstations and weakly encrypted LM hashes were being stored in the SAM database. This combination of weak password enforcement, synchronization, and weak hash encryption threatens not only the accounts on the workstation but also opens the door to accounts in NDS.

Internet Explorer - According to the SANS top 20 list, the main vulnerabilities associated with IE are unpatched systems and weak security settings. Of these two it was discovered that unpatched systems presented a serious problem for us. Weak security setting were not a problem as they had been set on the clone and periodically rechecked. The main problem with keeping all systems patched and up-to-date was the time it took to test each patch and then install them to the workstations. Quite often machines would just be overlooked in the patch process, or due to work load, patches would not be rolled out in a timely manner. It was decided that a more effective and efficient patch management system needed to be implemented.

Windows Remote Access Services - The Top 20 list points to four types of vulnerabilities relating to remote access services:

- NetBIOS – Unprotected Windows Networking Shares
- Anonymous Logon - Null session vulnerabilities
- Remote Registry Access
- Remote Procedure Calls

Since we do not use Microsoft servers we do not install the Microsoft client. In addition, NetBIOS over TCP/IP is disabled on all workstations. This should negate any vulnerabilities associated with NetBIOS and unprotected Windows shares. To address "null session" vulnerabilities the RestrictAnonymous registry value had been set to "2" on all workstations several months prior, which effectively eliminates the Anonymous logon vulnerability.[16] An investigation of the remote registry access problem has been inconclusive because the tools mentioned in the Top 20 document require Windows NT, which we do not have. Given this uncertainty, this vulnerability must be considered a threat and mitigation efforts taken. RPC vulnerabilities are closely tied to patch management and will be considered a threat until new patch management procedures are in place.[17]

---

[15] Ball, p. 9. A nice examination of NetWare's password policy weaknesses prior to NMAS and SecureLogin.

[16] Microsoft.

[17] "The best way by far is to apply the relevant patches..." as stated in the SANS Top 20 List section on protecting against RPC vulnerabilities.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Windows Script Hosting - Windows script hosting is enabled on all workstations in order to run several in-house .vbs scripts. This vulnerability must be considered a threat until mitigated.

Risk assessment

At this point in the analysis we had defined and prioritized the threats to our system and assessed the most common vulnerabilities used to exploit those threats. Each threat had been classified as a high, medium, or low level of concern and a short list of vulnerabilities had been identified. To assess our level of risk for each threat we simply needed to decide if a vulnerability could be used to produce a threat and, if so, assign a level of risk based on the level of concern.

Risk (High, Medium , Low) =Threat (High, Medium , Low) X Vulnerability (Yes/No)

As discussed earlier, each of the five relevant vulnerabilities identified in Table 2 could be exploited on our system. If exploited, each vulnerability could be used by itself or in combination with another to produce any one of the threats identified in Table 1. Therefore, since each threat can be produced by any one of the relevant vulnerabilities we could make an assessment of risk in each of the following areas:

High Risk
Systems used as launching pads

Medium Risk
System downtime
Destruction of electronic assets

Low Risk
Modification of electronic assets
Theft of electronic assets

Mitigation Measures

To help define our countermeasures it was decided that each must meet the following criteria:

They must be cost neutral - Budget restrictions at the time of this assessment prohibited the expenditure of any additional funds for this project. Any countermeasures that were to be implemented were to be done at no additional monetary cost to the department.

They must be focused and effective - Rather than trying to implement grand procedures to address every aspect of each risk, it was decided to focus on limited groups of

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

measures which would address the most vulnerable aspect of each risk.

They must be efficient - Implementation and maintenance must not be overly burdensome. Security procedures are much less likely to be successful if they are complicated and time consuming.

Given these criteria, three countermeasures were identified that addressed each of the relevant vulnerabilities. As seen in Table 2, several of the countermeasures helped mitigate more than one threat. This overlap or "layering" is one of the foundations of defense in-depth and helped validate the selection of the countermeasure. In addition, it illustrated the efficiency of the measure. Below is a discussion of the final countermeasures and the implementation issues associated with each.

Single Sign-on - This countermeasure was implemented to address the problem of weak passwords and password synchronization discussed in the *Windows Authentication* section on vulnerabilities. Included in the latest version of the free Novell Client for Microsoft (version 4.9) were components of Novell's SecureLogin technology.[18] One of these components is SecretStore which enables Novell's implementation of single sign-on at the client level.[19] Once enabled on the client, and the client is authenticated to NDS, the single sign-on process prompts the user for an application's authentication credentials. In our case, Windows 2000 would prompt the user for the user's Windows ID and password. SecretStore then encrypts the Windows password and stores it in the registry where it can be passed to Windows on subsequent logins.[20] This is quite different from our old policy of letting the client synchronize the password and solved the problem of storing NDS passwords in the SAM database.

I then leveraged this technology to enforce strong Windows passwords by changing the user's workstation password to be a very strong 28+ character passphrase which includes upper/lower case and special characters. Once set, the user is asked to log into NDS as normal. After authenticating to NDS the user is prompted for the Windows passphrase. At this point an administrator who knows the passphrase must enter it for the user. Subsequent logins are then handled by the Novell client which, after NDS authentication, supplies the passphrase to Windows. At this point an extremely good password has been enforced on the Windows account and

[18] Novell2.

[19] Mashayekhi.

[20] Novell3, Fix 1. While this TID states that the password is stored in the registry it does not specify the type of encryption used. One might assume that 168-bit 3DES is used as described in Novell2 in the section describing remote and mobile users.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

the user can continue to use the familiar password policies enforced by NDS. The same user passphrase is used for all user accounts and known only to myself. It is also contained in a sealed envelope and securely stored with other account information according to department procedures.

Several disadvantages to this procedure must be mentioned. First, an administrator who knows the standard passphrase must be present the first time a user logs on. This is not seen as an issue since the department is small, users typically use only one machine, and workstations are usually in place for several years before replacement. Second, while NDS passwords are set to expire every 30 days, the Windows passphrase have been set to never expire. This was done to prevent Windows from prompting the user to change the workstation password. While this is definitely not a "best practices" procedure, it was felt that the benefit of guaranteeing a very strong password on the workstation outweighed the remote possibility that it might somehow be discovered by an attacker. I am evaluating the option of using Windows password policies to set the Windows password to expire in 30 days, setting the minimum length requirement to 28 characters with complexity, and training the users to type a random strong passphrase when prompted. The user will then be free from remembering the Windows passphrase because Novell's SecureLogin will pass it to windows for authentication.

Security Templates - Applying security templates was selected as a countermeasure because they are easy to configure, very powerful, and are available from security groups who have customized them for specific security needs. After reviewing and testing the templates from Microsoft, NSA, and the Center for Internet Security (CIS), I decided to choose the CIS Win2kProGold_R1.2.4 template.[21] This template specifically provides countermeasures for the anonymous logon issues[22] and remote registry access[23] vulnerabilities discussed in *Windows Remote Access Services* section of the Top 20 list. In addition it provides defense in-depth against Windows Script Hosting exploits, windows authentication weaknesses, and possibly IE and MDAC exploits by tightening NTFS access permissions.

While the security improvements provided by this template are far to many to discuss here, there are several which directly mitigate the problem of LM hashes. First the template checks to make sure that the LAN Manager Authentication Level is set to "Send NTLMv2 response only". This will prevent the workstation from using the weaker LM hash during authentication.[24] Second I modified the template to add

---

[21] CIS.

[22] CIS2, p. 25, Section 3.1.1.

[23] CIS2, p. 40, Section 4.1.10.

[24] CIS2, p. 28, Section 3.2.1.16

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

HKLM\system\currentcontrolset\control\lsa\nolmhash=1 to the registry to prevent the LM hash from being stored in the registry. This setting should remove LM hashes from the registry after the passwords are changed.[25] In addition, the template removes all rights to debug privileges (SeDebugPrivilege). One benefit of this setting is that pwdump2, a utility that dumps password hashes from the SAM database for later cracking, will not work without access to this privilege.[26]

Two modifications were required to make this template work in our environment. Both involved registry settings designed to block denial of service attacks against the workstation. Below are the two registry modifications made by the default template:

HKLM\system\currentcontrolset\services\tcpip\parameters\enablepmtudiscovery = 0

HKLM\system\currentcontrolset\services\tcpip\parameters\synattackprotect=2

Disabling MTU discovery prevents an attacker from negotiating the MTU size down therefore causing unnecessary fragmentation and a possible denial of service. For some reason, connections across our routers would eventually time out if MTU discovery was disabled. This setting was modified to allow discovery. Setting the SynAttackProtect value to 2 caused a shrinking window size problem to occur for connections across our routers. Setting the value to 1 fixed this problem. The fully modified template can be found in Appendix 1.

Windows Automatic Updates - Each of the vulnerabilities identified in Table 2 can be mitigated completely or in part by an effective patch management strategy. As stated above, we needed to implement a more timely and consistent method for distributing patches. After reviewing many procedures for rolling out patches it was decided that either Windows Automatic Updates[27] or Software Update Services[28] would meet our needs.

Windows "Automatic Updates" is a feature that can be enabled from the control panel to automatically contact a Windows Update server on the Internet and download critical updates. Updates can be scheduled to run at various intervals with the choice of notifying the user, just downloading, or downloading and installing the updates as they become available. While this is a very convenient way to keep our workstations patched to Microsoft's standards, I was hesitant to enable the feature without being able to test the patches first.

---

[25] SANS, Section W3.5, Topic 6

[26] Sabin.

[27] Microsoft3.

[28] Microsoft4.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

I investigated Microsoft's Software Update Services as an alternative to automatic updating. This product enables you to set up your own Windows Update Server and select the updates to distribute to your clients. Although the product showed great promise, one of its requirements is that it must be run on a Windows 2000 Server or later. Since one of the criteria for adopting a procedure was that it had to be cost free, I was forced to abandon the project due to the cost of purchasing the server license.

This led me to revisit the Windows Automatic Updates service. After several years of downloading patches, testing, and installing them on each individual machine I had only encountered one patch which caused a conflict. At this point, it seemed like the advantages of having automatic and timely updates outweighed the possibility that a patch would cause an application to fail. If an update did cause a problem, it would be an easy task to manually uninstall that particular patch on each workstation. It was also possible to specify a time during which the uploads would occur as not to disrupt people during working hours or tying up bandwidth. The system would even reboot a machine should a patch require it. After testing a few machines and being satisfied with the results, I decided that the benefits of using the service finally outweighed the risks.

One disadvantage was that the Automatic Updates feature required the Client for Microsoft Networks. Prior to this, the client was not installed on the network which precluded many of the vulnerabilities associated with the software. This turned out to be only a minor concern since the client could be installed yet disabled without breaking the update service.

After

Windows Authentication - Password security at the Windows level has been improved significantly. Weak windows passwords have been completely removed from the system as have LM hashes from the SAM database. The system ensures that Windows user account passwords are now 28 character passphrases containing upper, lower, and special characters. In fact, the users do not even know their Windows account passwords. In addition, NDS and Windows passwords are no longer synchronized. The Novell client can now authenticate the user to Windows without prompting them for passwords. The single sign-on countermeasures were implemented with no additional cost to the department and required very little maintenance after the initial setup stage.

NDS password weaknesses are still a problem and improvement efforts are ongoing. While user education is an ongoing process, password monitoring may be a more fruitful avenue to pursue. Using tools such as Pandora to do proactive checking for weak NDS passwords may be one means of helping enforce our policies.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Security templates - By modifying the CIS Win2kProGold_R1.2.4 template I was able to create a template which address a multitude of known vulnerabilities. As a precaution, the custom security template was only applied to a handful of workstations in the main office. The custom template was applied to each computer using the Microsoft Security Configuration and Analysis tool. To date, no further difficulties have been encountered with the template. After several more weeks of testing these templates will be distributed to all remaining workstations using the SecEdit utility and logon scripts. With the exception of a few minor changes, these machines have been hardened to a level that meets consensus agreement while mitigating many of the vulnerabilities identified in this study.

Windows Automatic Updates - Enabling Automatic Updates has been an enormous time saver. Patches are now downloaded and installed during the night when activity is at a minimum. Other software such as service packs and version upgrades are not installed by this service. This gives administrators the flexibility to install the service packs and upgrades which typically require more testing. To date, no unintended side effects have been seen as a result of enabling this service.

To monitor the patches a Microsoft utility called Qfecheck is run from the logon scripts.[29] This produces a report which lists the hotfixes installed on the machine. The utility also checks to make sure that the hotfix is installed correctly. By scanning through these logs it is easy to determine if a machine is not updating correctly.

Conclusion

The challenges of securing even a small department may at times seem to be a monumental task. This is especially true for system administrators who cannot dedicate as much time to security issues as they may wish. Information security demands a level of knowledge and effort that is sometimes hard to incorporate into a busy schedule. Perimeter defenses may lull us into a false sense that our systems are safe. The expected costs of improved security may be more than management is willing to spend. Given barriers such as these, it may be seem questionable as to whether security improvements are worth it. In this case study I have tried to demonstrate that a systematic approach to identifying threats and vulnerabilities can be used to identify and implement efficient and cost-effective countermeasures with a minimal amount of time and money. With the mantra of “defense in-depth” as a guide, I hope to have significantly improved the security posture of my department.

[29] Microsoft5

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

References List

Ball, Erik. “Password security and the means of achieving it within a Novell environment”. GSEC v.1.4b. February 3, 2003. URL:http://www.sans.org/rr/papers/index.php?id=909. (December 21, 2003)

Center for Internet Security (CIS). “Center for Internet Security Benchmarks and Scoring Tool for Windows 2000 and Windows NT”. October 2003. URL:http://www.cisecurity.org/bench_win2000.html. (December 21, 2003)

Center for Internet Security (CIS2). “Windows 2000 Professional Operating System Level 2 Benchmark Consensus Baseline Security Settings”. Version 2.0.5. September 02, 2003. Available for download at URL:http://www.cisecurity.org/sub_form.html. (December 21, 2003)

Mashayekhi, Cameron.“A Technical Overview of Novell SecretStore 3.2”. Novell AppNotes®. May 2003. URL:http://developer.novell.com/research/appnotes/2003/may/03/a030503.htm. (December 20, 2003)

Microsoft Corporation. ”How to Use the RestrictAnonymous Registry Value in Windows 2000". Microsoft Knowledge Base Article - 246261. URL:http://support.microsoft.com/default.aspx?scid=kb;en-us;246261&Product=win2000. (December 19, 2003)

Microsoft Corporation (Microsoft2). ”How to Prevent Windows from Storing a LAN Manager Hash of Your Password in Active Directory and Local SAM Databases”. Microsoft Knowledge Base Article - 299656 . URL:http://support.microsoft.com/default.aspx?scid=kb;en-us;299656. (December 20, 2003)

Microsoft Corporation (Microsoft3). ”HOW TO: Schedule Automatic Updates in Windows XP, Windows 2000, or Windows Server 2003”. Microsoft Knowledge Base Article - 327838. URL:http://support.microsoft.com/default.aspx?scid=kb%3Ben-us%3B327838. (January 20, 2004)

Microsoft Corporation (Microsoft4). ”Software Update Services Overview White Paper”. URL:http://www.microsoft.com/windowsserversystem/sus/susoverview.mspx. (January 20, 2004)

Microsoft Corporation (Microsoft5). ”Qfecheck.exe Verifies the Installation of Windows 2000 and Windows XP Hotfixes”. Microsoft Knowledge Base Article - 282784 . URL:http://support.microsoft.com/default.aspx?scid=kb;en-us;282784&Product=win2000. (December 20, 2003)

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

National Institute of Standards and Technology (NIST). “Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories”. Version 1.0. December 2003. URL:http://csrc.nist.gov/publications/drafts/draft-sp800-60V1.pdf. (December 20, 2003)

Novell Security Alerts (Novell). URL:http://support.novell.com/filefinder/security/indexc.html. (December 20, 2003)

Novell, Inc. (Novell2).“Novell® SecureLogin: Novell Nsure™Secure Identity Management -Technical White Paper”. URL:http://www.novell.com/collateral/4621348/4621348.html. (December 20, 2003)

Novell, Inc. (Novell3).“No option to synchronize Windows password with 4.9 client - TID10081981”. September 4, 2003. URL:http://support.novell.com/cgi-bin/search/searchtid.cgi?/10081981.htm. (December 20, 2003)

Sabin, Todd. “PWDUMP2". URL:http://razor.bindview.com/tools/desc/pwdump2_readme.html. (December 20, 2003)

SANS Institute (SANS). “The Twenty Most Critical Internet Security Vulnerabilities (Updated) ~ The Experts Consensus”. Version 4.0. October 8, 2003. URL:http://www.sans.org/top20/. (December 20, 2003)

SANS Institute Reading Room (SANS RR). URL:http://www.sans.org/rr/catindex.php?cat_id=39. (December 20, 2003)

Simple Nomad. “Novell NetWare 5.x Security Guide”. April, 2001. URL:http://www.bindview.com/resources/WhitePapers/NW_5SecurityGuideWP.pdf.(December 20, 2003)

United States General Accounting Office (GAO), Accounting and Information Management Division. “Information Security Risk Assessment - Practices of Leading Organizations”. November 1999. URL:http://www.gao.gov/special.pubs/ai00033.pdf.(December 20, 2003)

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Appendix 1 - Modified CIS Win2kProGold_R1.2.4.inf Security Template

```
;-----------------------------------------------------------------------------

; Security Configuration Template for Security Configuration Editor
;
; Template Name:       Mod5_Win2kProGold_R1.2.4.inf
;
; Modified:     11/15/2003 spf
;
;-----------------------------------------------------------------------------

[Unicode]
Unicode=yes
[Version]
signature="$CHICAGO$"
Revision=1
[Profile Description]
Description=Windows 2000 Professional Security Settings
[System Access]
MinimumPasswordAge = 1
MaximumPasswordAge = -1
MinimumPasswordLength = 28
PasswordComplexity = 1
PasswordHistorySize = 24
LockoutBadCount = 3
ResetLockoutCount = 15
LockoutDuration = 15
RequireLogonToChangePassword = 1
ForceLogoffWhenHourExpire = 1
ClearTextPassword = 0
[System Log]
MaximumLogSize = 81920
AuditLogRetentionPeriod = 0
RestrictGuestAccess = 1
[Security Log]
MaximumLogSize = 81920
AuditLogRetentionPeriod = 0
RestrictGuestAccess = 1
[Application Log]
MaximumLogSize = 81920
AuditLogRetentionPeriod = 0
RestrictGuestAccess = 1
[Event Audit]
AuditSystemEvents = 3
AuditLogonEvents = 3
```

© SANS Institute 2004, Author retains full rights.

AuditObjectAccess = 2
AuditPrivilegeUse = 2
AuditPolicyChange = 2
AuditAccountManage = 3
AuditAccountLogon = 3
[Registry Values]
users\.default\software\microsoft\windows\currentversion\policies\explorer\nodrivetypeautorun=4,149
machine\system\currentcontrolset\services\tcpip\parameters\tcpmaxhalfopenretried=4,80
machine\system\currentcontrolset\services\tcpip\parameters\tcpmaxhalfopen=4,100
machine\system\currentcontrolset\services\tcpip\parameters\synattackprotect=4,1
machine\system\currentcontrolset\services\tcpip\parameters\performrouterdiscovery=4,0
machine\system\currentcontrolset\services\tcpip\parameters\keepalivetime=4,300000
machine\system\currentcontrolset\services\tcpip\parameters\enablepmtudiscovery=4,1
machine\system\currentcontrolset\services\tcpip\parameters\enableicmpredirect=4,0
machine\system\currentcontrolset\services\tcpip\parameters\enabledeadgwdetect=4,0
machine\system\currentcontrolset\services\tcpip\parameters\disableipsourcerouting=4,2
machine\system\currentcontrolset\services\netlogon\parameters\signsecurechannel=4,1
machine\system\currentcontrolset\services\netlogon\parameters\sealsecurechannel=4,1
machine\system\currentcontrolset\services\netlogon\parameters\disablepasswordchange=4,0
machine\system\currentcontrolset\services\netbt\parameters\nonamereleaseondemand=4,1
machine\system\currentcontrolset\services\mrxsmb\parameters\refusereset=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\hidden=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\autosharewks=4,0
machine\system\currentcontrolset\services\lanmanserver\parameters\autodisconnect=4,30
machine\system\currentcontrolset\services\ipsec\nodefaultexempt=4,1
machine\system\currentcontrolset\services\cdrom\autorun=4,0
machine\system\currentcontrolset\control\session manager\protectionmode=4,1
machine\system\currentcontrolset\control\session manager\memory management\clearpagefileatshutdown=4,1
machine\system\currentcontrolset\control\print\providers\lanman print services\servers\addprinterdrivers=4,1
machine\system\currentcontrolset\control\lsa\restrictanonymous=4,2

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

machine\system\currentcontrolset\control\lsa\lmcompatibilitylevel=4,3
MACHINE\System\CurrentControlSet\Control\lsa\NoLMHash=4,1
machine\system\currentcontrolset\control\lsa\fullprivilegeauditing=3,0
machine\system\currentcontrolset\control\lsa\auditbaseobjects=4,0
machine\system\currentcontrolset\control\crashcontrol\autoreboot=4,0
machine\software\microsoft\windows\currentversion\policies\system\shutdownwithoutlogon=4,0
machine\software\microsoft\windows\currentversion\policies\system\legalnoticetext=1,This system is for the use of authorized users only. Individuals using this computer system without authority,or in excess of their authority,are subject to having all of their activities on this system monitored and recorded by system personnel. Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity,system personnel may provide the evidence of such monitoring to law enforcement officials.
machine\software\microsoft\windows\currentversion\policies\system\legalnoticecaption=1,--- 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\currentversion\policies\network\nodialin=4,1
machine\software\microsoft\windows\currentversion\policies\network\hidesharepwds=4,1
machine\software\microsoft\windows\currentversion\policies\explorer\nodrivetypeautorun=4,255
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=1,1
machine\software\microsoft\windows nt\currentversion\winlogon\autoadminlogon=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\windows nt\currentversion\aedebug\auto=4,0
machine\software\microsoft\non-driver signing\policy=3,1
machine\software\microsoft\drwatson\createcrashdump=4,0
machine\software\microsoft\driver signing\policy=3,1
[Group Membership]
*S-1-5-32-547__Memberof =
*S-1-5-32-547__Members =
[Registry Keys]
1="classes_root", 2,

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

```
"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)(A;CI;KR;;;BU)"
2="machine\software", 2,
"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)(A;CI;KR;;;BU)S:AR(AU;OICIFA;K
A;;;WD)"
3="machine\software\microsoft\netdde", 2, "D:PAR(A;CI;KA;;;BA)(A;CI;KA;;;SY)"
4="machine\software\microsoft\os/2 subsystem for nt", 2,
"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)"
5="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)"
6="machine\software\microsoft\windows nt\currentversion\perflib", 2,
"D:AR(A;CI;KR;;;IU)(A;CI;KA;;;BA)(A;CI;KA;;;SY)(A;CIIO;KA;;;CO)"
7="machine\software\microsoft\windows\currentversion\group policy", 0,
"D:PAR(A;CI;KA;;;BA)(A;CI;KR;;;AU)(A;CI;KA;;;SY)"
8="machine\software\microsoft\windows\currentversion\installer", 0,
"D:PAR(A;CI;KA;;;BA)(A;CI;KA;;;SY)(A;CI;KR;;;BU)"
9="machine\software\microsoft\windows\currentversion\policies", 0,
"D:PAR(A;CI;KA;;;BA)(A;CI;KR;;;AU)(A;CI;KA;;;SY)"
a="machine\system", 2,
"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)(A;CI;KR;;;BU)S:AR(AU;OICIFA;K
A;;;WD)"
b="machine\system\clone", 1, "D:AR"
c="machine\system\controlset001", 0,
"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)(A;CI;KR;;;BU)"
d="machine\system\controlset002", 0,
"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)(A;CI;KR;;;BU)"
e="machine\system\controlset003", 0,
"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)(A;CI;KR;;;BU)"
f="machine\system\controlset004", 0,
"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)(A;CI;KR;;;BU)"
10="machine\system\controlset005", 0,
"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)(A;CI;KR;;;BU)"
11="machine\system\controlset006", 0,
"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)(A;CI;KR;;;BU)"
12="machine\system\controlset007", 0,
"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)(A;CI;KR;;;BU)"
13="machine\system\controlset008", 0,
"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)(A;CI;KR;;;BU)"
14="machine\system\controlset009", 0,
"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)(A;CI;KR;;;BU)"
15="machine\system\controlset010", 0,
"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)(A;CI;KR;;;BU)"
16="machine\system\currentcontrolset\control\securepipeservers\winreg", 2,
"D:PAR(A;CI;KA;;;BA)"
17="machine\system\currentcontrolset\control\wmi\security", 2,
"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)"
```

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

```
18="machine\system\currentcontrolset\enum", 1,
"D:PAR(A;CI;KR;;;BA)(A;CI;KR;;;AU)(A;CI;KA;;;SY)"
19="machine\system\currentcontrolset\hardware profiles", 0,
"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)(A;CI;KR;;;BU)"
1a="machine\system\currentcontrolset\services\snmp\parameters\permittedmanagers",
2, "D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)"
1b="machine\system\currentcontrolset\services\snmp\parameters\validcommunities", 2,
"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)"
1c="users\.default", 2,
"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)(A;CI;KR;;;BU)"
1d="users\.default\software\microsoft\netdde", 2, "D:PAR(A;CI;KA;;;BA)(A;CI;KA;;;SY)"
1e="users\.default\software\microsoft\protected storage system provider", 1, "D:AR"
[File Security]
1="c:\", 0,
"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)S:
AR(AU;OICIFA;FA;;;WD)"
2="c:\autoexec.bat", 2, "D:PAR(A;;FA;;;BA)(A;;FA;;;SY)"
3="c:\boot.ini", 2, "D:PAR(A;;FA;;;BA)(A;;FA;;;SY)"
4="c:\config.sys", 2, "D:PAR(A;;FA;;;BA)(A;;FA;;;SY)"
5="c:\documents and settings", 0,
"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)"
6="c:\documents and settings\administrator", 2,
"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
7="c:\documents and settings\all users", 0,
"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)"
8="c:\documents and settings\all users\documents\drwatson", 2,
"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)(A;OICIIO;DCLCWP;;;BU)(
A;OICI;CCSWWPLORC;;;BU)"
9="c:\documents and settings\default user", 2,
"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)"
a="c:\io.sys", 2, "D:PAR(A;;FA;;;BA)(A;;FA;;;SY)"
b="c:\msdos.sys", 2, "D:PAR(A;;FA;;;BA)(A;;FA;;;SY)"
c="c:\ntbootdd.sys", 2, "D:PAR(A;;FA;;;BA)(A;;FA;;;SY)"
d="c:\ntdetect.com", 2, "D:PAR(A;;FA;;;BA)(A;;FA;;;SY)"
e="c:\ntldr", 2, "D:PAR(A;;FA;;;BA)(A;;FA;;;SY)"
f="c:\program files", 2,
"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)"
10="c:\program files\resource kit", 2, "D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
11="c:\program files\resource pro kit", 2, "D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
12="c:\winnt", 2,
"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)"
13="c:\winnt\$ntservicepackuninstall$", 2, "D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
14="c:\winnt\config", 2, "D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
15="c:\winnt\csc", 2, "D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
16="c:\winnt\debug", 0,
"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)"
```

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

```
17="c:\winnt\debug\usermode", 0,
"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)(A;;CCDCWP;;;BU)(A;OIIO;DCLC;;;BU)"
18="c:\winnt\offline web pages", 2, "D:(A;OICI;GA;;;WD)"
19="c:\winnt\regedit.exe", 2, "D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
1a="c:\winnt\registration", 0, "D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)(A;OICI;FR;;;BU)"
1b="c:\winnt\repair", 2, "D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
1c="c:\winnt\security", 2, "D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)"
1d="c:\winnt\system32", 2,
"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)"
1e="c:\winnt\system32\appmgmt", 0,
"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)"
1f="c:\winnt\system32\at.exe", 1, "D:PAR(A;;FA;;;BA)(A;;FA;;;SY)"
20="c:\winnt\system32\dllcache", 2,
"D:AR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)"
21="c:\winnt\system32\dtclog", 2,
"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)"
22="c:\winnt\system32\grouppolicy", 0,
"D:PAR(A;OICI;FA;;;BA)(A;OICI;0x1200a9;;;AU)(A;OICI;FA;;;SY)"
23="c:\winnt\system32\ias", 2,
"D:AR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)"
24="c:\winnt\system32\ntbackup.exe", 2, "D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
25="c:\winnt\system32\ntmsdata", 0, "D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
26="c:\winnt\system32\rcp.exe", 2, "D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
27="c:\winnt\system32\regedt32.exe", 2, "D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
28="c:\winnt\system32\reinstallbackups", 1,
"D:AR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)(A;OICI;0X1200A9;;;PU)"
29="c:\winnt\system32\rexec.exe", 2, "D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
2a="c:\winnt\system32\rsh.exe", 2, "D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
2b="c:\winnt\system32\secedit.exe", 2, "D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
2c="c:\winnt\system32\setup", 0,
"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)"
2d="c:\winnt\system32\spool\printers", 2,
"D:AR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)(A;OICI;0X1000ad;;;BU)"
2e="c:\winnt\tasks", 2, "D:AR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)"
[Service General Setting]
1="alerter", 4,
"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;RPWPDTRC;;;SY)"
2="browser", 4,
"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;RPWPDTRC;;;SY)"
3="clipsrv", 4,
"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;RPWPDTRC;;;SY)"
4="fax", 4,
"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;RPWPDTRC;;;SY)"
5="iisadmin", 4,
"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;RPWPDTRC;;;SY)"
6="messenger", 4,
```

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;RPWPDTRC;;;SY)"
7="mnmsrvc", 4,
"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;RPWPDTRC;;;SY)"
8="msftpsvc", 4,
"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;RPWPDTRC;;;SY)"
9="remoteaccess", 4,
"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;RPWPDTRC;;;SY)"
a="remoteregistry", 4,
"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;RPWPDTRC;;;SY)"
b="sharedaccess", 4,
"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;RPWPDTRC;;;SY)"
c="smtpsvc", 4,
"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;RPWPDTRC;;;SY)"
d="snmp", 4,
"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;RPWPDTRC;;;SY)"
e="snmptrap", 4,
"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;RPWPDTRC;;;SY)"
f="tlntsvr", 4,
"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;RPWPDTRC;;;SY)"
10="w3svc", 4,
"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;RPWPDTRC;;;SY)"
[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 = *S-1-5-32-546
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 =
senetworklogonright =
seprofilesingleprocessprivilege = *S-1-5-32-544
seremoteshutdownprivilege = *S-1-5-32-544
serestoreprivilege = *S-1-5-32-544
sesecurityprivilege = *S-1-5-32-544

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

```
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
```

© SANS Institute 2004, Author retains full rights.

Last Updated: September 4th, 2015

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Crystal City 2015	Crystal City, VAUS	Sep 08, 2015 - Sep 13, 2015	Live Event
SANS Network Security 2015	Las Vegas, NVUS	Sep 12, 2015 - Sep 21, 2015	Live Event
SANS Seoul 2015	Seoul, KR	Sep 14, 2015 - Sep 19, 2015	Live Event
SANS Tallinn 2015	Tallinn, EE	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Baltimore 2015	Baltimore, MDUS	Sep 21, 2015 - Sep 26, 2015	Live Event
Data Breach Investigation Summit & Training	Dallas, TXUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Perth 2015	Perth, AU	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS ICS Amsterdam 2015	Amsterdam, NL	Sep 22, 2015 - Sep 28, 2015	Live Event
SANS Bangalore 2015	Bangalore, IN	Sep 28, 2015 - Oct 17, 2015	Live Event
SANS Seattle 2015	Seattle, WAUS	Oct 05, 2015 - Oct 10, 2015	Live Event
SANS DFIR Prague 2015	Prague, CZ	Oct 05, 2015 - Oct 17, 2015	Live Event
SOS: SANS October Singapore 2015	Singapore, SG	Oct 12, 2015 - Oct 24, 2015	Live Event
SANS Tysons Corner 2015	Tysons Corner, VAUS	Oct 12, 2015 - Oct 17, 2015	Live Event
SANS Gulf Region 2015	Dubai, AE	Oct 17, 2015 - Oct 29, 2015	Live Event
SANS Tokyo Autumn 2015	Tokyo, JP	Oct 19, 2015 - Oct 31, 2015	Live Event
SANS Cyber Defense San Diego 2015	San Diego, CAUS	Oct 19, 2015 - Oct 24, 2015	Live Event
SANS Sydney 2015	Sydney, AU	Nov 09, 2015 - Nov 21, 2015	Live Event
SANS South Florida 2015	Fort Lauderdale, FLUS	Nov 09, 2015 - Nov 14, 2015	Live Event
SANS London 2015	London, GB	Nov 14, 2015 - Nov 23, 2015	Live Event
Pen Test Hackfest Summit & Training	Alexandria, VAUS	Nov 16, 2015 - Nov 23, 2015	Live Event
SANS Hyderabad 2015	Hyderabad, IN	Nov 24, 2015 - Dec 04, 2015	Live Event
SANS Cape Town 2015	Cape Town, ZA	Nov 30, 2015 - Dec 05, 2015	Live Event
SANS San Francisco 2015	San Francisco, CAUS	Nov 30, 2015 - Dec 05, 2015	Live Event
Security Leadership Summit & Training	Dallas, TXUS	Dec 03, 2015 - Dec 10, 2015	Live Event
SANS Milan 2015	OnlineIT	Sep 07, 2015 - Sep 12, 2015	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced