Global Information Assurance Certification Paper

Disclaimer

This paper was written for the purpose of the Auditing Windows NT Servers Practical to show evidence that the Auditing tools have been implemented. The information in the document may not have the same results at other organizations, and in no means is to be used as a public guideline. Third party software was used to provide evidence of such Auditing practices where applicable.

Section 1 – User Accounts – NT User DataBase

The Windows NT SAM contains all the user / computer account information such as passwords , last login date and time , credentials for accounts and can be a very powerful thing if it was to fall into the wrong hands. Therefore, reasonable measures should be employed to maintain the security of this data.

Account Management

Background Information

User Manager for Domains enables you to manage security for domains and computers. This includes creating and managing user accounts and groups, and managing the domain's security policies such as accounts, user rights, auditing and trust relationships.

To better manage a large number of user accounts, you could utilize a tool such as "Unused Account Ferret" to do accounting on your SAM.

Unused accounts are network accounts that have not been logged onto for a specified period of time. Accounts often become unused when the person to whom the account belongs leaves the organization and there is no procedure in place to assure they are deactivated or deleted.

Risks

Unused accounts:

Provide a means of unauthorized access - Individuals who have left an organization should not have access to network resources, especially any employee or contractor who has left in dispute.
Are a prime target for brute-force attacks - Password expiration policies will have no effect on unused accounts because there is nobody logging onto them. This gives a cracker enough time to complete a brute-force attack on a previously captured password hash.
Cost money - Depending on the licensing model, unused accounts are likely to mean unused software licenses. This can lead to substantial increases in cost, especially if

server licensing information is used to calculate application license requirements. (Source: http://www.tpis.com.au/products/uaf/default.htm)

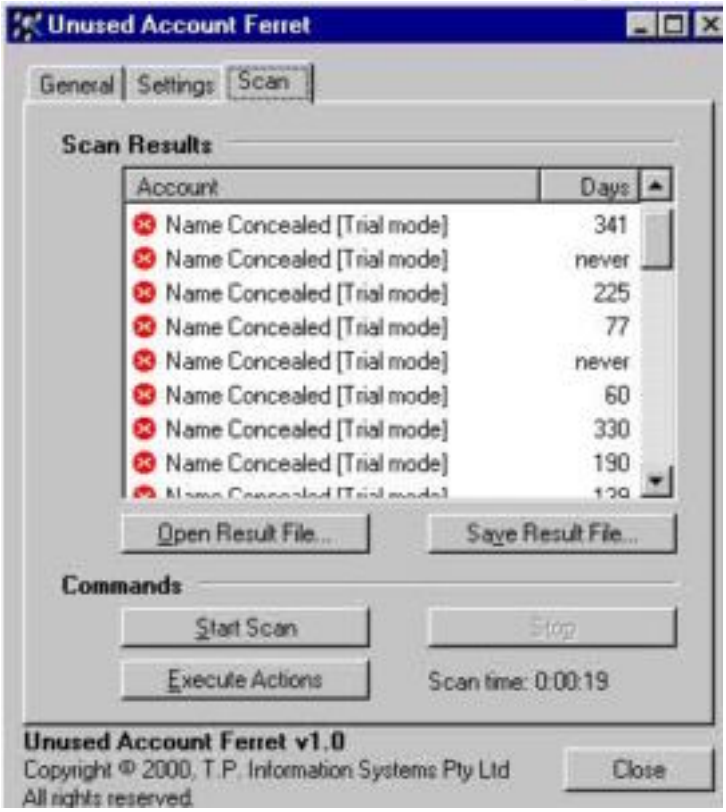
Pre-Implementation

This program was installed on the PDC. Based on your companies security policy you set the auto disable , delete warnings for user accounts.

Development

1. After installing "Unused Account Ferret". You will have to configure your options.
   - Domain controllers (accurate number of DC's)
   - Number of Query threads
   - Settings – Actions (delete, disable)

2. After this is completed. You can start your scan. Results screenprint below.
   Note: User names are not displayed.



Conclusion

Although Unused Account Ferret can help to rid your network of unused accounts in minutes, Administrators should still be notified when a user is dismissed, or will be away for a lengthy leave of absence.

Password Policy

Passwords are security measures used to restrict logon names to user accounts and access computer systems and resources. A password is a unique string of characters that must be provided before a logon name or an access is authorized.

A violation is an infraction committed willfully and with complete lack of regard for legal, moral, or ethical considerations. That's why measures are taken to prevent attackers from accessing our users ID's to gain unprivileged access to our network.
In all cases passwords are the final and in some cases only line of defense against security violations.

Risks

Hackers find weak password to compromise our network security using several methods. Password Policy Enforcer helps us create a base of harder to crack passwords by setting limitations for our end-users.

Background Information

Microsoft provides a password filtering tool free of charge in Sp3 and beyond in the form of "Passfilt". The major drawback with Passfilt is that the criteria is set by Microsoft and non adjustable. Adjustment would require you to custom program your own password filtering Library. Password Policy Enforcer 2.4 by TPIS is a user customizable Password Filtering Dynamic Link Library which allows the administrator to fully customize password policies based on your companies Security policy.

Pre-Implementation

Before implementation of any software you should fully test it in a development environment before moving it into live production systems.

Development

1. Based on your Companies Security Policy determine the criteria needed .

2. Screen print below shows how you choose the appropriate limitations.

3. Password complexity is forced through this program so that when a user changes passwords so they must meet the following policy:

   a. Passwords must not contain: Username (GTurner), Fullname or Bi-directional
   b. Must contain Alpha (a-z), Numeric (0-9), Mixed Case (at least 3 unique characters).
   c. When you're prompted for your new password, it must be different from your old password, with a similarity of only 3 characters.
   d. Passwords must be between 8-14 characters long**.**

4. After password policy is implemented on all DC's, the client portion must be copied to each machine. (Copy config.cfg command via login scripts)

5. PPE (Password Policy Enforcer) replicates to all DC's

6. Administrators should test to see if the policy displays the correct violation message. If the administrator enters an invalid password, PPE will display a message that tells you exactly limitations you are lacking.

Conclusion

Password Policy enforcer is enabled and fully functioning as required.
Another security measure implemented to help maintain a secure system.

Registry Changes

Background

Prior to Windows NT 4.0 Service Pack 4 (SP4), Windows NT supported two kinds of challenge/response authentication:

- LanManager (LM) challenge/response
- Windows NT challenge/response (also known as NTLM challenge/response)

Windows NT also supported session security mechanisms that provided for message confidentiality and integrity.

Risks

To allow access to servers that only support LM authentication, Windows NT clients prior to SP4 always use both, even to Windows NT servers that supported NTLM authentication. LM authentication is not as strong as NTLM or NTLMv2 because the algorithm allows passwords longer than 7 characters to be attacked in 7 character chunks. This limits the effective password strength to 7 characters drawn from the set of uppercase alphabetic, numeric, and punctuation characters, plus 32 special ALT characters. Users often do not even avail themselves of anything more than alphabetic characters.

In contrast, NTLM authentication takes advantage of all 14 characters in the password and allows lowercase letters. Thus, even though an attacker eavesdropping on the Windows NT authentication protocol can attack it in the same way as the LM authentication protocol, it will take far longer for the attack to succeed. If the password is strong enough, it will take a single 200 MHz Pentium Pro computer an average of 2,200 years to find the keys derived from it and 5,500 years to find the password itself (or 2.2 years and 5.5 years with 1,000 such computers, and so forth). [1]

Development

After Insuring Sp4 or higher installed

1. Run Registry Editor (Regedt32.exe).
2. From the HKEY_LOCAL_MACHINE subtree, go to the following key:

[1] Microsoft KnowledgeBase Article Q147706 – Disabling Lan Man Authentication

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa

3. Click Add Value on the Edit menu.

4. Add the following values:

   Value Name: LMCompatibilityLevel
   Data Type: REG_DWORD
   Data: 0 (default) to 5 as defined above

5. From the HKEY_LOCAL_MACHINE subtree, go to the following key:

   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0

6. Click Add Value on the Edit menu.

7. Add the following values:

   Value Name: NtlmMinClientSec
   Data Type: REG_DWORD
   Data: 0 (default) or as defined above

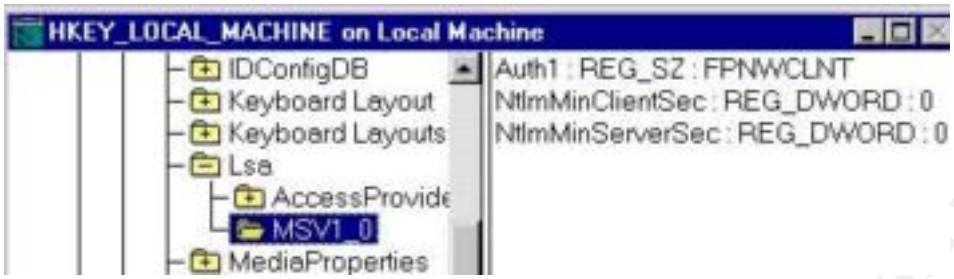
   Value Name: NtlmMinServerSec
   Data Type: REG_DWORD
   Data: 0 (default) or as defined above

8. Click OK and then quit Registry Editor.

9. Shut down and restart Windows NT.

Screenprint before registry changes:

Screenprint after registry changes:



Conclusion

Passwords contained within the SAM are now protected to a higher level against brute force tools such as L0phtCrack

Section 2 – Host Based Auditing

Background

With any operating system there exists an amount of potential security hazards and applications that may compromise system integrity. Host based auditing will allow the administrator to minimize these risks through best practices.

Service Packs

Service packs are the means by which Windows NT product updates are distributed. Service packs keep the product current, and extend and update your computer's functionality. Service packs include updates, system administration tools, drivers, and additional components. All are conveniently bundled for easy downloading. Service packs are cumulative -- each new service pack contains all the fixes in previous service packs, as well as any new fixes. You do not need to install a previous service pack before you install the latest one. (Source: Knowledgebase article ID:Q152734)

Risks

Every time a new service pack is released Microsoft tells us the security holes that have been resolved. As long as your service pack version is known, chance of exploitation exists. Whenever there is a configuration change to a server, the service pack needs to be re-installed (re-applied), to maintain the necessary security.

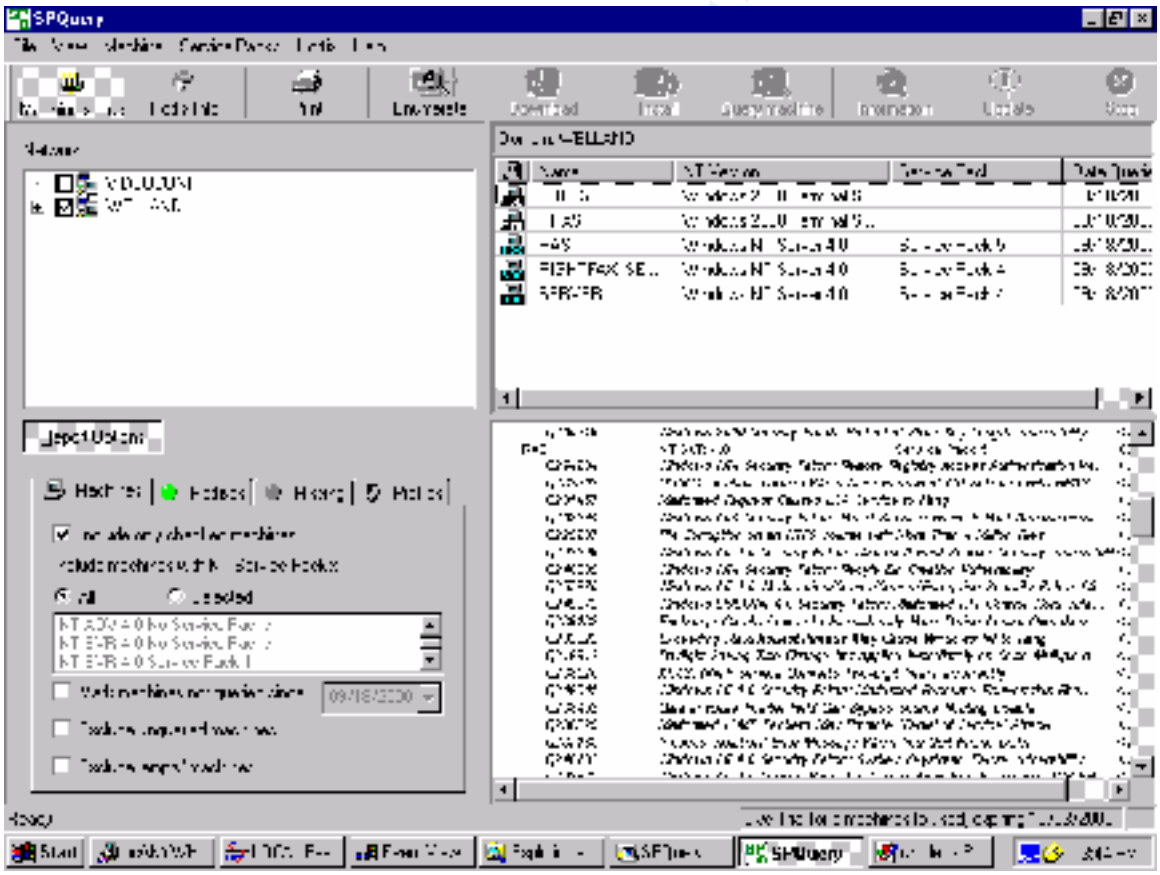
Pre-Implementation: All software packages / software updates etc. should be first run on a development system. Proven stable, the software package /hot fix should then be put into a live environment.

Development:

1. Service packs are the Number one security feature that should be updated to try and prevent known security holes. Service Packs (updates) and Hot fixes (updates between service packs) should be updated upon each release.

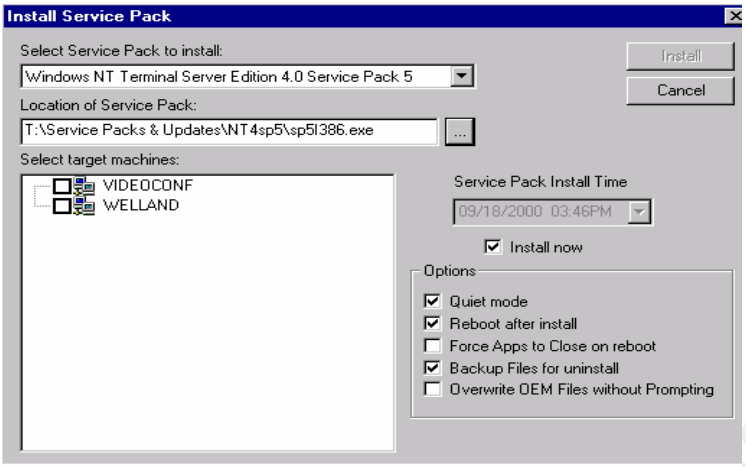
SPQuery by St. Bernard Software is a hot fix and service pack security management utility that eliminates the confusion and labor of maintaining hot fixes and service packs on NT 4.0 and Win2000 systems.

Screenprint:



1. After installing SPQuery, you will have to configure which servers (machines) will have to be monitored.

2. When configurations are set, go to Help->Update on the toolbar. This will gather the lastest service pack / hot fix information.



Conclusion

SPQuery monitors and informs the administrators when a new service pack or hot fix is released. SPQuery is a great enterprise tool. You can install any service pack to any computer on the domain.

Machine Audit Log Policy

Managing audit logs is critical. When a Windows NT audit logs fills up, you can either erase the data and continue operation, or it can halt the system. To check event logs, you can setup AT to run audits via batch, then dump the log (using dumpel) to a centralized server. In addition, you can use third party tools, such as Enterprise Monitor, to watch for specific event ID's which signify full logs and spawn a log rotation process.

Note: Maintaining good Event logs in the event of an attack are critical as these may provide some insight into areas affected ,or ways that security breaches happen.

Risks

If you have no secure area to store your event logs, an intruder can cause the log to fill up to hide evidence of his/her actions. An audit logs allows administrators to track the actions of all users, valid or not.

Pre-Implementation

Make sure all Audit events are enabled. The checklist below is used to ensure all servers are setup for audit logging on a medium security network.

Development

1. In the Event Viewer, pull down the Log Menu and use the log settings…option to set the log file size very large to avoid running out of log space while setting up the system and/or audit policy.

2. Determine the network policy that best suits the needs of your company

3. Under User Manager for Domains –> Polices –>Audit Policy. Check which polices that you want to log. Screenprint below

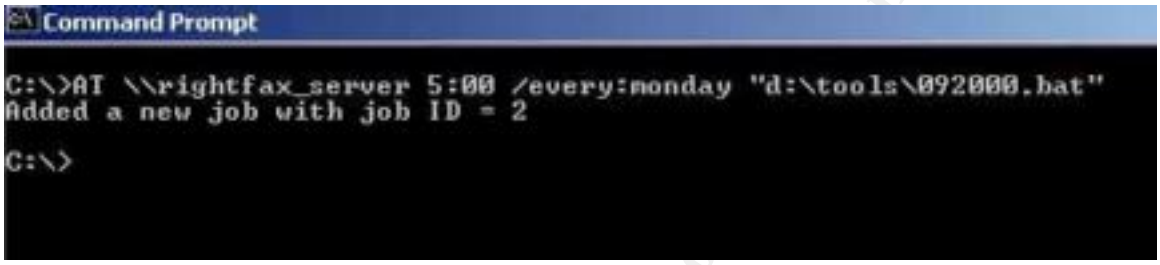
4. A checklist was developed to track events on each server.

Server	Welland (File server)	Niagara	Grimsby	Thorold
Control Item				
Logon and Logoff Success	Enabled	Enabled	Enabled	Enabled
Logon and Logoff Failure	Enabled	Enabled	Enabled	Enabled
File and Object Access-Success	Enabled	Disabled	Enabled	Disabled

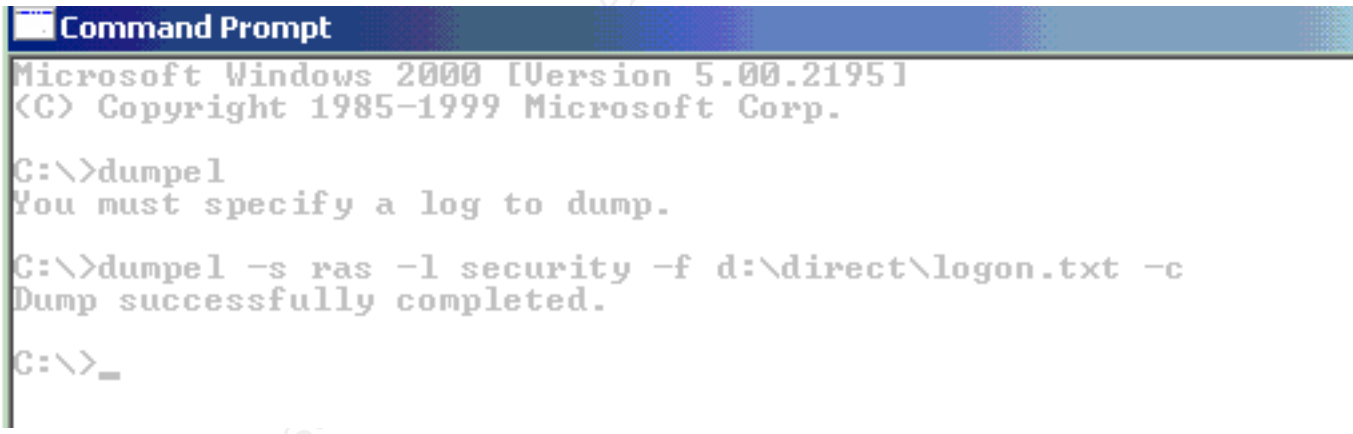
Server	Welland (File server)	Niagara	Grimsby	Thorold
Control Item				
File and Object Access - Failure	Enabled	Disabled	Enabled	Disabled
Use of User Rights - Success	Enabled	Disabled	Disabled	Disabled
Use of User Rights - Failure	Enabled	Disabled	Disabled	Disabled
User and Group Management – Success	Enabled	Enabled	Disabled	Disabled
User and Group Management – Failure	Enabled	Enabled	Disabled	Disabled
Security Policy Changes – Success	Enabled	Enabled	Enabled	Enabled
Security Policy Changes – Failure	Enabled	Enabled	Enabled	Enabled
Restart, Shutdown and System – Success	Enabled	Enabled	Enabled	Enabled
Restart, Shutdown and System - Failure	Enabled	Enabled	Enabled	Enabled
Process Tracking- Success	Enabled	Disabled	Enabled	Disabled
Process Tracking- Failure	Enabled	Disabled	Enabled	Disabled

- All Severs are control enabled according to our policy.
- No resources are being accessed on disabled items.
- The Polices stated above may not meet the needs of other security networks.

5. Setup AT at a command prompt to run audits via batch.



6. Get a dump of the security log. Place it in a secure centralized location.



7. Below is a sample output from Dumpel.exe.

9/15/2000,4:06:20 PM,8,2,528,Security,NIAGARA\Administrator,,RAS,Successful Logon: User Name: Administrator Domain: NIAGARA Logon ID: (0x0,0x323179) Logon Type: 3 Logon Process: KSecDD Authentication Package: MICROSOFT_AUTHENTICATION_PACKAGE_V1_0 Workstation Name: \\thorold
9/15/2000,4:11:14 PM,8,2,528,Security,NT AUTHORITY\ANONYMOUS LOGON,,RAS,Successful Logon: User Name: Domain: Logon ID: (0x0,0x3247E5) Logon Type: 3 Logon Process: NtLmSsp Authentication Package: MICROSOFT_AUTHENTICATION_PACKAGE_V1_0 Workstation Name: domaincontroller

8. After system has been in operation for a couple of weeks, the file size can be reset to a smaller value.

Conclusion

Even when security auditing is enabled, administrators still must review the logs for any abnormalities. Logs should be reviewed on a regular basis, daily or weekly, depending on the size of your network.
Alerts and third party monitors help the administrator detect abnormalities faster.

Note: Do not choose "clear log manually", since this can cause the system to come to a halt, causing DOS (Denial of Service).

Permission Changes to Event Log Settings

By default the event logs are readable by everyone with full control over the contents. Change these to applicable settings as per policy.

Auditing with Sysdiff

Background Information

Sysdiff is a tool that helps administrators automate the install process of software. Sysdiff takes a snapshot of the registry and file system. For the purpose of auditing, we are only going to look at Sysdiff's ability to snapshot the system and report any changes. Third party tools which do the same type thing would be a product such as "TripWire".

Risks

You will want to skip temp files and exclude files that are open during your audit to ensure that sysdiff gets a complete image. Open files will cause Sysdiff to abort.

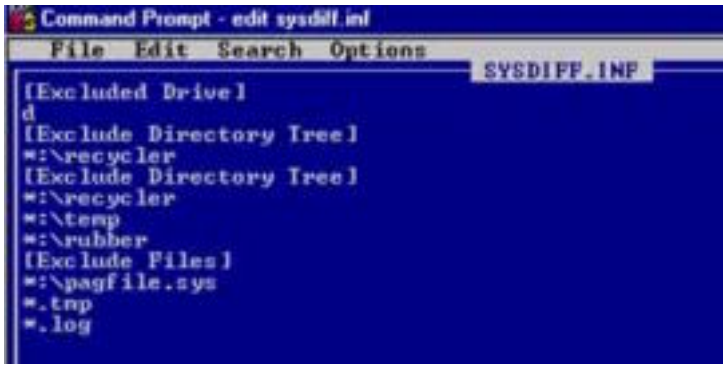
Pre-Implementation

Before using Sysdiff you should download the latest version from Microsoft's FTP site. You will also what to verify which directories and files you want to include in your baseline.

Development

1. Editing Sysdiff.inf

   Once you know which directories you want to record, you will want to edit the Sysdiff.inf file.
   Make sure you have good commentary so that you can use the same .inf file for several machine. Example screenprint below.



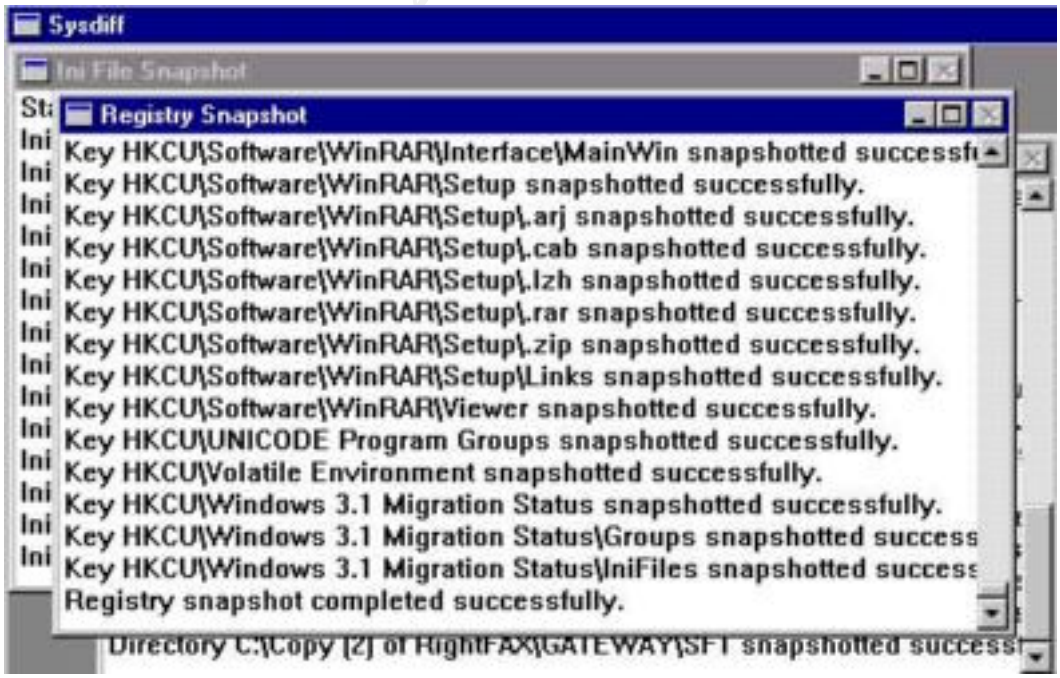
2. Comparing with Sysdiff.

Using sysdiff to edit is a three-step process.

- You will have to run Sysdiff with the "snap" switch to create a baseline
- To compare the system setup to the original baseline file later, you will have to use "diff" command.
- To produce a different file later, you will have to use the "dump" switch.

a. At the command prompt, execute the following command to get a snapshot of the registry:
C:\> sysdiff /snap imame.img

Screenprint:



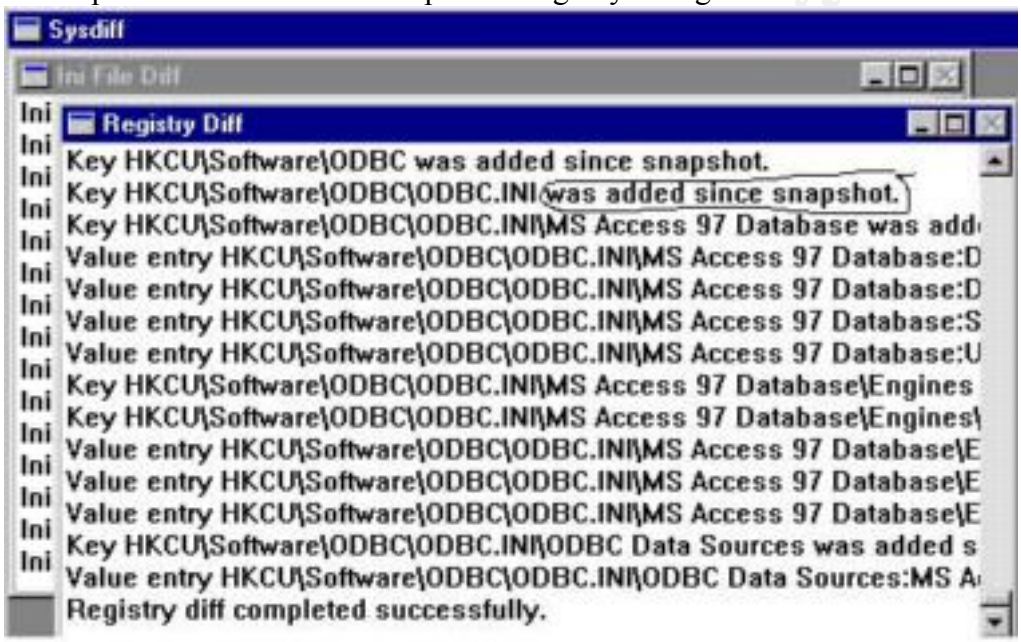
b. Install a software package so that you can compare snapshots. (Microsoft Project 98)

c. At the command prompt, execute the following command to compare snapshots

C:\>sysdiff /diff image.img diff.img

d. Check the current system against the original image.

Screenprint: Circled is an example of a registry change



e. You can output changes into a readable form.
At the command prompt, execute the following:
C:\>sysdiff /dump diff.img diff.txt

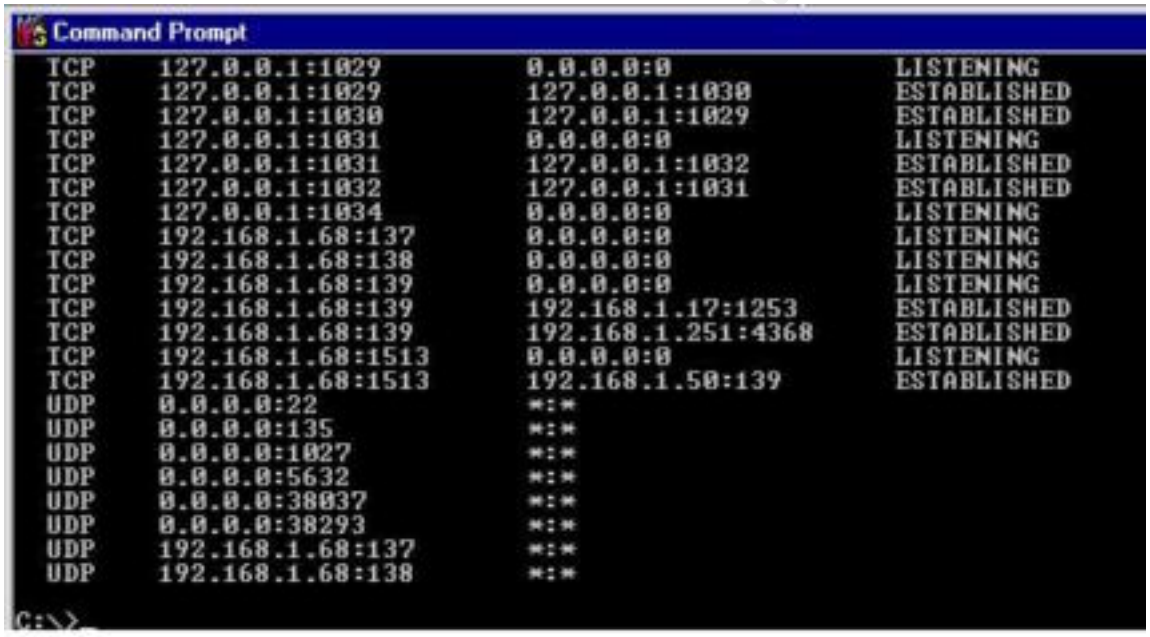
3. Baseline: Registry only
   - You can use regdump.exe to create an ASCII version of the registry
   - Values change normally
   - Try and run a few baselines to determine what exactly is "normal"

Service Auditing

Utilizing tools such as Netstat , Inzider on the host will give you output on what ports your machine is listening for connections on.

Netstat –na

Screenprint of output from the command C:\netstat –na



You should be positively able to answer why every port is being listened on.

To find out port number assignments, you can refer to:
(**ftp://ftp.isi.edu/in-notes/iana/assignments/port-numbers**)

Section 3 – Reference Materials

Appendix A – Security Policy in Effect for this Auditing Process

i. All User Accounts must meet the Password Policy of:
ii. 8-14 Characters in Length, Containing at least one of each of the following Upper and Lower Case, Numerics, Special Characters. There must also be at least 3 unique characters in the string
iii. Passwords must not contain username, full name or any combination of.
iv. Password History will be retained for 5 changes
v. Change Interval is 30 days

1. All Systems with Resources being shared will have full auditing turned on.

2. Event Logs are readable only by Domain Admin / System accounts with dumps of the logs being stored to central secured location

3. All System Times Synced against master timeserver for Domain.

4. Systems should be using NTLM v2 for Authentication and session setup with Lan Manager Authentication Disabled

5. Unneeded Services should be uninstalled / removed . (ie WWW , Ftp)

6. Once System has been installed Baselines generated before put into Production

7. User Accounts not in use for over 30 days become disabled. Accounts over 60 flagged for deletion.

REFERENCES

Brenton. Chris. Auditing Windows NT. Basic Windows NT Auditing. The SANS Institute, 2000.

Fossen, Jason, and Kolde, Jennifer. Securing Windows NT: Step-by-Step. The SANS Institute GIAC Training, 2000.

Glaser, JD. Intrusion Auditing Under Windows NT. NT Objectives Inc., 1999

"How to Enable NTLM 2 Authentication for Windows 95/98/2000 and NT." Microsoft Knowledge Base Article ID: Q239869

"How to Disable LM Authentication on Windows NT." Microsoft Knowledge Base Article ID: Q147706

"How to Obtain the Latest Windows NT 4.0 Service Pack." Microsoft Knowledge Base Article ID: Q152734

IANA. Port Assigments. Retrieved form World Wide Web.
(ftp://ftp.isi.edu/in-notes/iana/assignments/port-numbers)

SANS Institute. Windows NT Security Step by Step. The SANS Institute, 1999.

TPIS. Products. Retrieved from World Wide Web.
(http://www.tpis.com.au/products/uaf/default.htm)

Last Updated: July 21st, 2017

Upcoming Training

SANSFIRE 2017	**Washington, DC**	**Jul 22, 2017 - Jul 29, 2017**	**Live Event**
SANS Virginia Beach 2017	**Virginia Beach, VA**	**Aug 21, 2017 - Sep 01, 2017**	**Live Event**
SANS Network Security 2017	**Las Vegas, NV**	**Sep 10, 2017 - Sep 17, 2017**	**Live Event**
SANS vLive - SEC505: Securing Windows and PowerShell Automation	**SEC505 - 201709,**	**Sep 18, 2017 - Nov 13, 2017**	**vLive**
Secure DevOps Summit & Training	**Denver, CO**	**Oct 10, 2017 - Oct 17, 2017**	**Live Event**
SANS San Francisco Winter 2017	**San Francisco, CA**	**Nov 27, 2017 - Dec 02, 2017**	**Live Event**
San Francisco Winter 2017 - SEC505: Securing Windows and PowerShell Automation	**San Francisco, CA**	**Nov 27, 2017 - Dec 02, 2017**	**vLive**
SANS Cyber Defense Initiative 2017	**Washington, DC**	**Dec 12, 2017 - Dec 19, 2017**	**Live Event**
SANS Southern California- Anaheim 2018	**Anaheim, CA**	**Feb 12, 2018 - Feb 17, 2018**	**Live Event**
SANS OnDemand	**Online**	**Anytime**	**Self Paced**
SANS SelfStudy	**Books & MP3s Only**	**Anytime**	**Self Paced**