



Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permitted without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Securing Windows and PowerShell Automation (Security 505)"
at <http://www.giac.org/registration/gcwn>

Richard D. Laboris
November 6, 2000

**GIAC SECURING WINDOWS
PRACTICAL ASSIGNMENT
Version 1.5**

Network Security 2000

Option 1 - Developments in auditing NT

This document outlines the steps involved in a typical NT Network audit. Each step includes some background information as well as procedures and tools available to assist with the audit. All work was performed on a Windows NT 4.0 Server with Service Pack 4 acting as a PDC.

Step 1:

Assess NT Network Domain Architecture:

Background Information:

The first step in any security audit should be to gather information about the systems, domains, and trusts on the network. This provides a big picture of the communication paths that are required and those that must be secured. A truly detailed audit will encompass all server and workstation accounts, files, and shares.

Risks:

A network is only as secure as its weakest link. Any unsecured host on a network can potentially give an attacker access to other, secured resources. Trivial passwords, modems, and unsecured documents on a workstation or server can create an entry point to your network.

Implementation:

The built-in *net* command provides much of the needed information.

To list all the domains (and workgroups) in the network, at the command prompt of the Server, type:

net view /domain

Output:

Developments in Auditing NT by: Richard D. Laboris

Domain

```
-----  
-  
FINANCE  
HUMAN_RESOURCES  
QUALITY  
ENGINEERING  
INFORMATION_TECHNOLOGY  
INTERNET  
INTRANET  
SECURITY  
YOUR_WORKGROUP  
TESTCORP_MASTER  
The command completed successfully.
```

Next, to obtain a list of all hosts in each domain from above, type **net view /domain: finance** (where **finance** is each domain name from above)

Output:

Server Name	Remark
-------------	--------

```
-----  
-  
\\ADMINISTRATOR  
\\HUMANRESOURCE  
\\MOKRADWEBSTER  
\\WKCANACOAT  
\\WKCANBICTRAIN6  
\\WKCANBICTRAIN_1  
\\WKCANCHAMLIN  
\\WKCANCJULITA  
\\WKCANCMCDERMOTT  
\\WKCANCNOBLE  
\\WKCANCPERRON  
\\WKCANCSR1  
\\WKCANCTASA  
\\WKCANCTASA1  
\\WKCANDBENNETT  
\\WKCANDCDANIEL  
The command completed successfully.
```

This information can be redirected to a file for later analysis and policy enforcement.

Next, using the Windows NT Resource Kit tool *nltest*, the domain controllers for a given domain can be enumerated:

nltest /dclist: finance

Output:

```
List of DCs in Domain finance
    \\SVFINANCEFILE (PDC)
    \\SVFINANCEPDC
    \\SVFINANCEMAIL
The command completed successfully
```

Here we can see which system is the Primary Domain Controller (PDC) and which are Backups.

Now that the Primary Domain Controller has been discovered, its trust relationships should be identified, again using *nltest*.

nltest /server:svfinancefile /trusted_domains

Output:

```
Status = 3221225506 0xc0000022
STATUS_ACCESS_DENIED
```

Here we see that the command failed because we were not authenticated to the server. This is a good time to discuss an important NT built-in feature, the null session (Discussed in more detail in step 5). By default, NT includes a null user account that is used for some system functions. It is possible to “connect” to a system using the net use command and logging in as the null user (with null password):

net use \\svfinancefile\IPC\$ "" /user:""

This does not give us full rights to the system, however it effectively logs us in to the PDC and allows us to run the *nltest* command and some others with success.

nltest /server:svfinancefile /trusted_domains

Output:

```
Trusted domain list:
    TESTCORP_MASTER
The command completed successfully
```

Here, we see that the PDC trusts the domain TESTCORP_MASTER.

With all the information gathered thus far, we can begin to build a map of the NT domain architecture which will help identify vulnerabilities.

Step 2:

Audit User Accounts and Shares:

Background Information:

Once we obtain a list of all servers, we can individually audit Service Pack and Hotfix levels, user account and password policies, and file and share permissions. These audits are critical to minimize vulnerabilities to intrusions and attacks.

Risks:

Since operating system and software vendors rely on service packs and hotfixes to keep products current, it is crucial to keep up with the latest releases as soon as they are available. Once a vulnerability finding is made public (usually when a hotfix is available), any systems that are not updated become easy targets for hackers. It is equally important to ensure account passwords are non-trivial and frequently changed and that files and shares are properly secured. Using readily available tools, a hacker can brute force guess a password in a matter of minutes or hours if the account policy allows it.

Implementation:

Service Packs & Hotfixes

Traditionally, keeping up to date on NT service packs and hotfixes has been a tedious task. On regular intervals, the network administrator should check the Microsoft site:

<http://www.microsoft.com/TechNet/security/srvpckin.asp> for the latest service pack for each product and download that patch:

Service Pack Information

One of the most critical security best practices is to always stay up to date on all service packs. Service packs are well-tested, comprehensive collections of fixes – including security fixes. Following are the most recent service packs for many Microsoft products.

Windows NT® Family	Latest Service Pack
Windows® 2000 Professional, Server and Advanced Server	Service Pack 1
Windows 2000 Datacenter Server	No service packs released
Windows NT 4.0 Workstation, Server, and Server, Enterprise Edition	Service Pack 6a
Windows NT 4.0 Server, Terminal Server Edition	Service Pack 6
Windows 9x Family	Latest Service Pack

Here we see that for NT 4.0 Workstation and Servers, the latest Service Pack is 6a.

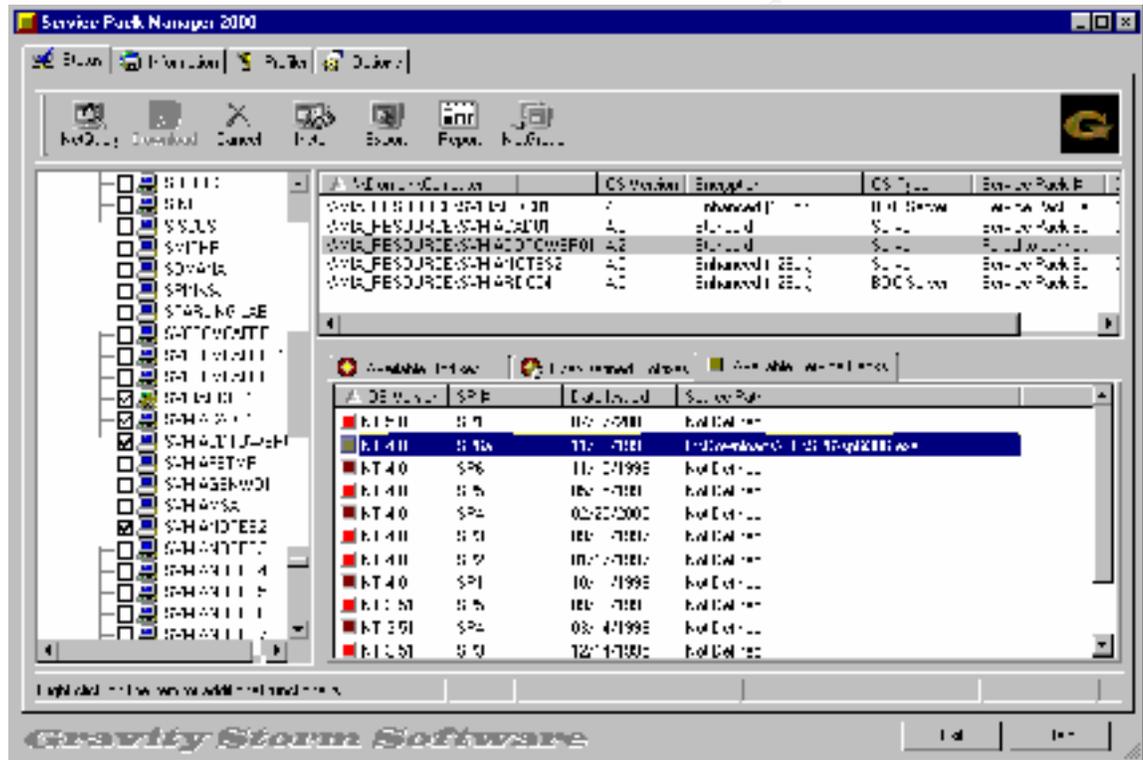
Then run *winver* (a built in utility) at the run prompt on each server to view NT version information including service pack and build level as shown below:

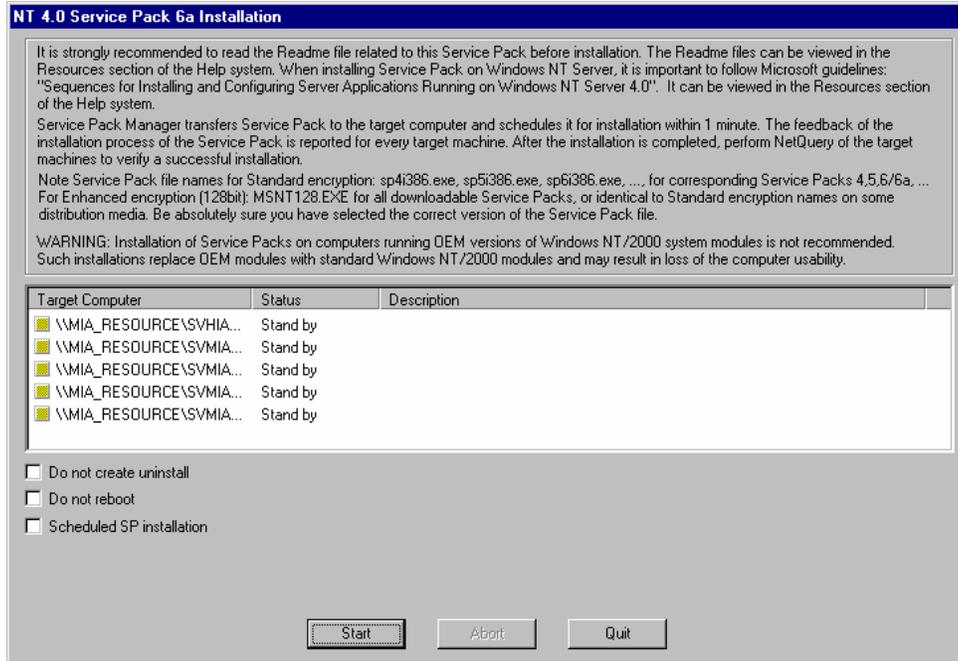


Check the Service Pack listed in the window against the latest version and upgrade if necessary. New tools are now available to facilitate in the

querying process such as “Service Pack Manager” by Gravity Storm Software (<http://home.sans.ir.com/gravitystorm>) and “SPQuery” by St. Bernard Software (<http://www.stbernard.com/spqproducts.html>).

Service Pack Manager provides a simple to use interface for administrating Service Packs. Upon startup, the software discovers all domains in your network. Once systems are selected in the network pane and the query is performed, system information including service pack level is displayed in the system pane. Below this, available service packs and hotfixes are displayed and may be downloaded and applied.



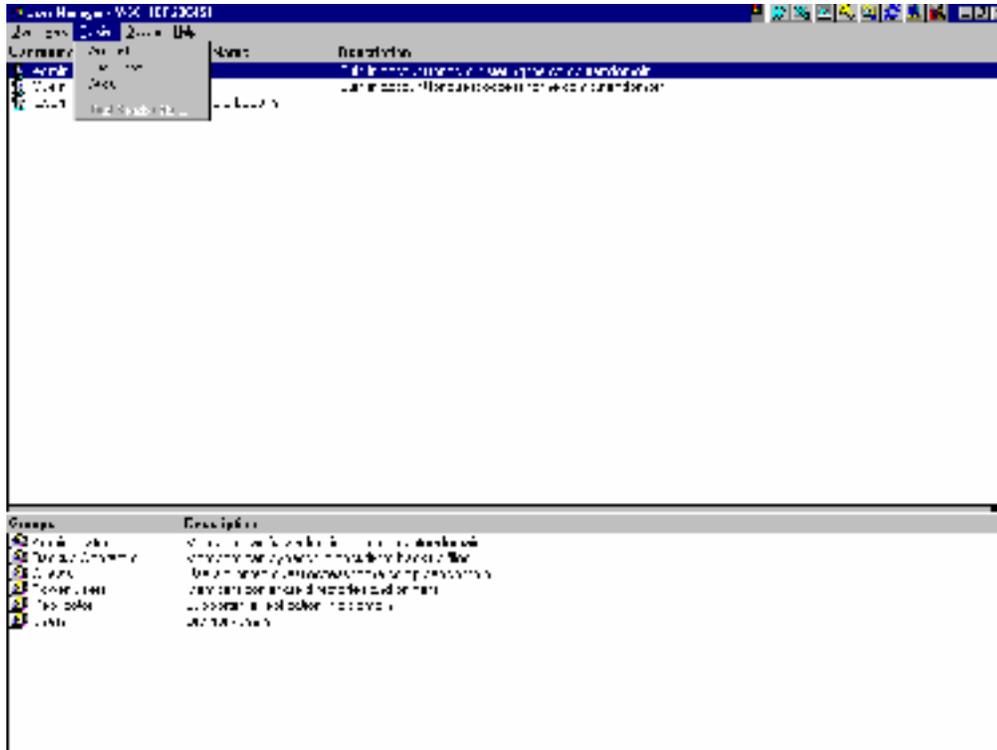


User Account and Password Policies

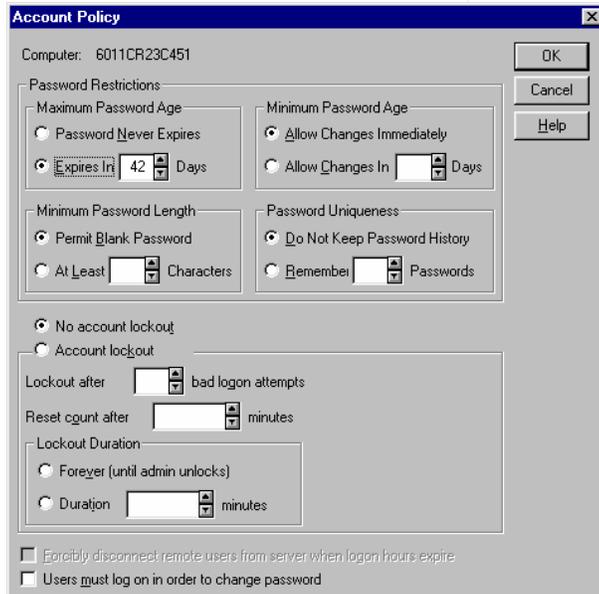
The combination of username and password is, in some cases, the only line of defense between a hacker and your network. For this reason it is important to make sure that policies are in place to prevent trivial usernames and passwords. NT has built in features for account policies that can be augmented with the use of third party utilities.

The NT User Manager for Domains tool contains a Policies Menu that allows for setting of Account, User Rights, and Audit policies.

© SANS Institute 2000 - 2002



The Account Policies Menu brings up the following dialog box:



This dialog box shows the account policy for the system (This information can also be obtained by using Pedestal Software's ntsec utility *ntuser* with the *policy* option):

The **Maximum Password Age** setting specifies a time limit for a password, after which a user must change the password. It is important to

specify a value such as 30 days. No maximum age allows a hacker unlimited time to learn and use a given password.

The **Minimum Password Age** setting specifies the minimum amount of time a password must be in effect before allowing changes. Setting this value to some minimum value prevents users from circumventing the password uniqueness setting (see below) by immediately cycling through passwords and back to the original.

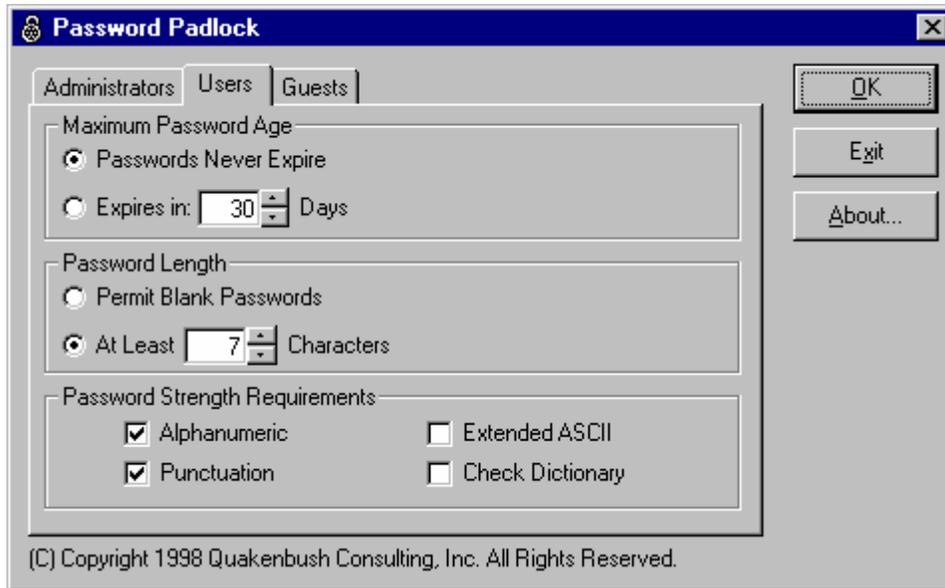
The **Minimum Password Length** setting specifies the minimum number of characters a password can be. It is recommended that passwords be at least 7 characters in length or more.

The **Password Uniqueness** setting specifies the number of passwords the user must use before being able to return to a given password. This, in conjunction with the Minimum Password Age, ensures that users don't reuse the same password over and over.

The **Account Lock Out** settings protect against password guessing by locking out an account after a specified number of attempts within a specified time period.

Another important step in account protection is for users to use strong passwords that are difficult to break. Some third-party tools are available that enforce these types of password checks. One such tool, *Quakenbush Password Padlock* (<http://www.quakenbush.com>), forces users to choose passwords with any combination of letters, numbers, punctuation, and extended ascii characters you specify.

Once installed, *Password Padlock* provides a control panel where all password filters are configured. Settings can be different for Administrators, Users, and Guests.

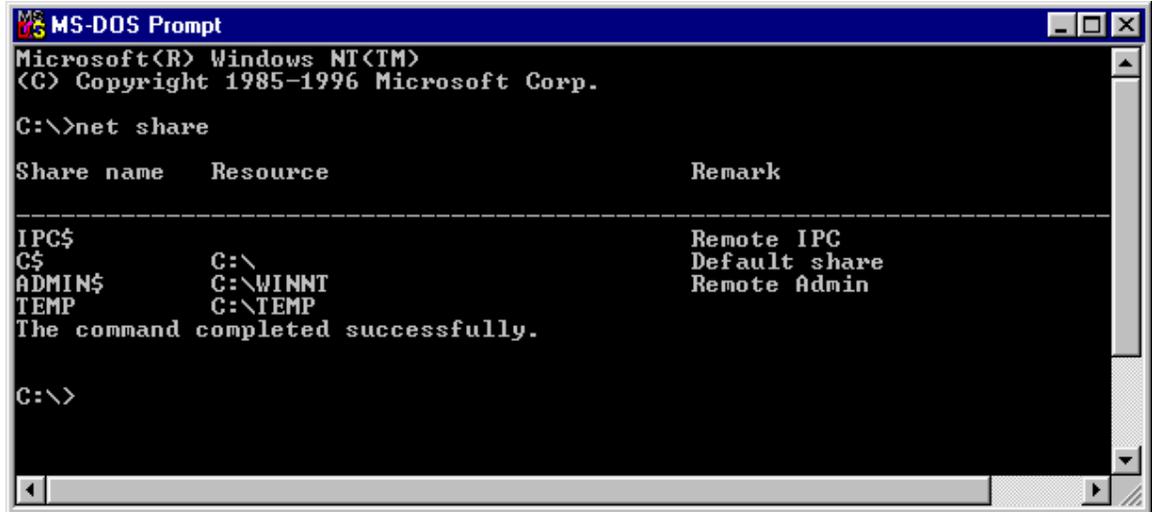


One downside to this tool is the cryptic error message displayed when a user attempts to enter a password that does not conform to the rules set:



File and Share Permissions

File level permissions only become an issue when someone has physical access to the system or remote access by way of shares. Therefore, it is critical that shares are audited and locked down so that only authorized users gain file level access. The built in NT command *net share* provides a listing of all shares running on a system including hidden shares and allows for creation or deletion of shares.



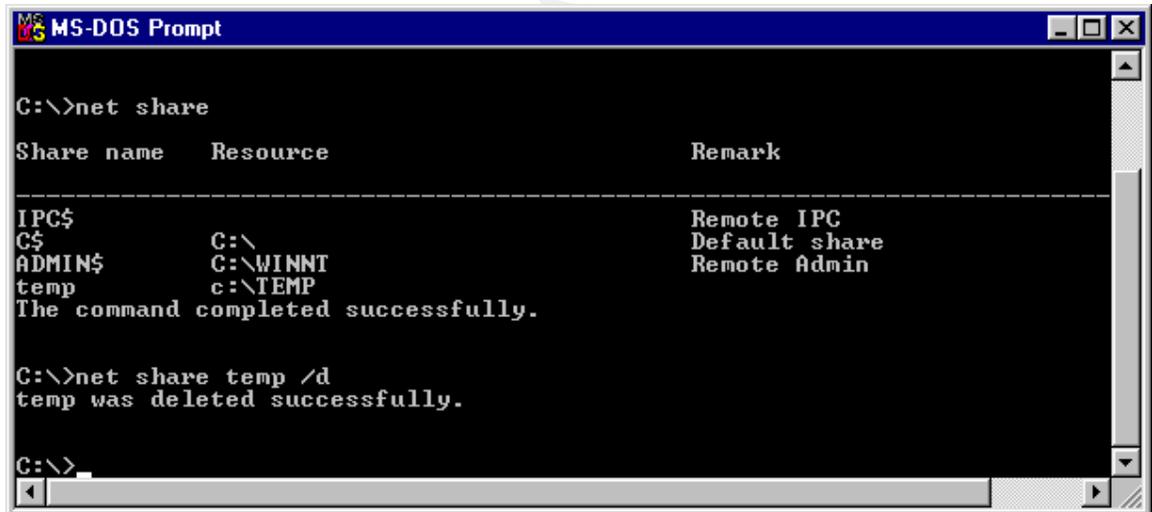
```
MS-DOS Prompt
Microsoft(R) Windows NT(TM)
(C) Copyright 1985-1996 Microsoft Corp.

C:\>net share

Share name      Resource                Remark
-----
IPC$            Remote IPC
C$              C:\                     Default share
ADMIN$          C:\WINNT                Remote Admin
TEMP            C:\TEMP
The command completed successfully.

C:\>
```

Shares that are not required (including default administrative shares), should be deleted by executing the `net share share_name /d` command as shown below:



```
MS-DOS Prompt

C:\>net share

Share name      Resource                Remark
-----
IPC$            Remote IPC
C$              C:\                     Default share
ADMIN$          C:\WINNT                Remote Admin
temp            c:\TEMP
The command completed successfully.

C:\>net share temp /d
temp was deleted successfully.

C:\>
```

In addition, prevent automatic creation of administrative shares (C\$, D\$, ADMIN\$) by setting the following in the Registry:

- ⊙ HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters\AutoShare Server

Set this value to 0.

Step 3:

Secure the User Account Database:

Background Information:

The SAM Database stores password hashes for domain and local computer accounts. This file is backed up onto the Operating System Partition and floppy disk when rdisk is executed. Although passwords are encrypted, the encryption scheme is weak because of backwards compatibility. Many utilities exist that can crack passwords from a SAM file using brute force.

Risks:

A hacker, who gains access to the SAM database files from the server or an emergency repair disk, can use a password-cracking tool to decipher the hashes and learn user passwords. Given enough time, most passwords in a given SAM file can be cracked. Even the trusted network administrator should not have access to user passwords. *L0phtcrack* from L0pht Heavy Industries (www.l0pht.com) is a password cracking program that can import a SAM file from and usually brute force crack all passwords within several hours.

Implementation:

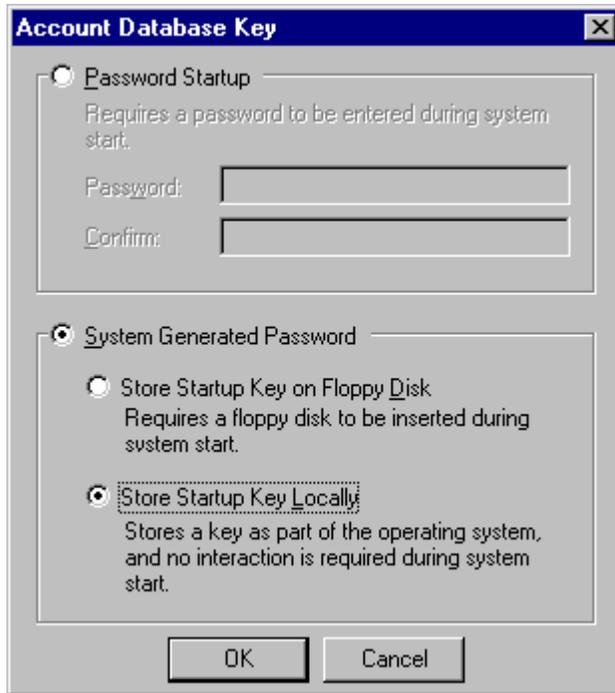
Securing the SAM database

The built-in *syskey* command provides the capability to use strong encryption techniques to increase protection of account password database. To enable *syskey*:

At a command prompt, execute: *syskey*. This opens the *syskey* window:



Select the "Encryption Enabled" radio button and click OK. The Account Database Key window will pop up. Here there are three options for protection:



- Use a machine-generated key as the System Key and store the key on the local system. This provides strong and allows for unattended system restart. At a minimum, all servers should use this encryption since it is transparent to users and administrators.
- Use a machine-generated key and store the key on a floppy disk. The floppy disk is required for the system to start and must be inserted when prompted after Windows NT begins the startup sequence, but before the system is available for users to logon. This is the most secure method as long as the floppy disk is stored in a secure place. This is also the most dangerous method since losing the floppy means having to reinstall the operating system.
- Use a password chosen by the Administrator. Windows NT will prompt for the password when the system is in the initial startup sequence, but before the system is available for users to logon.

Once you select the desired protection level, click OK. Upon restarting the system, syskey will be active.

Step 4:

Configure Audit Settings:

Background Information:

If, after all security settings are in place, a hacker still manages to gain access to your network, the only remaining course of action is auditing. Auditing user access to a system allows administrators to monitor all activity, whether authorized or not. This can be useful in detecting an intrusion as it occurs (with the help of intrusion detection systems) or in determining which security hole allowed penetration.

Risks:

A hacker who successfully penetrates a network, if undected, can wreak havoc until the damage begins to alarm network personnel. Only a properly audited network will quickly detect a suspicious user and allow time for countermeasures.

Implementation:

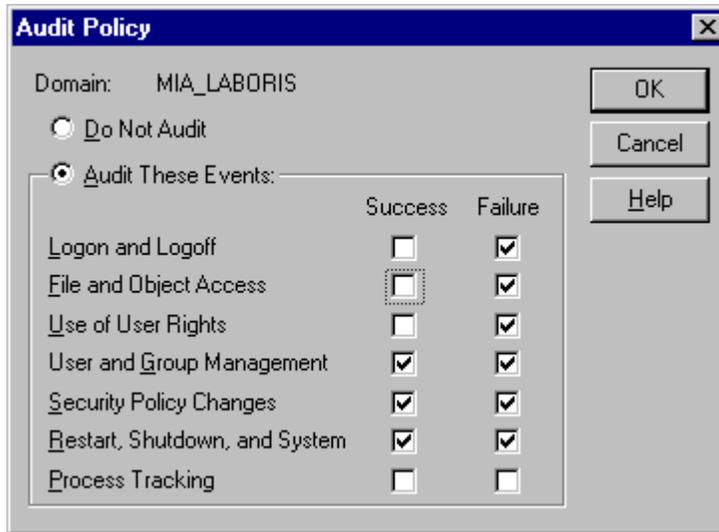
By default, auditing is not enabled. To enable auditing:

1. Launch User Manager for Domains
2. Select Policies...Audit... from the menu.
3. Select the radio button labeled "Audit These Events"
4. Now you have the option of selecting which events are audited. This setting will vary depending on server function and performance (since auditing requires some system resources). Below is Microsoft's recommended setting for servers by type (Effective Security Monitoring ,Chapter 4 from *Microsoft Windows NT 4.0 Security, Audit, and Control*, published by Microsoft Press):

<i>Audit Feature</i>	<i>Description</i>	<i>Domain Controller</i>	<i>RAS Server</i>	<i>File and Print</i>	<i>Data-base</i>	<i>Web Server</i>	<i>Work-station</i>
Logon and Logoff	Enables auditing of logon/off attempts, and breaking of network connections to servers.	Select Failure	Select Failure	Do not select	Select Failure	Do not select	Do not select
Use of User	Enables auditing of	Select Failure	Select Failure	Do not select	Do not select	Do not select	Do not select

Rights	attempts to user rights that have/have not been granted.						
User and Group Management	Enables auditing of creation, deletion, and modification of user and group accounts.	Select Success Select Failure	Select Success Select Failure	Do not select	Do not select	Do not select	Do not select
Security Policy Changes	Enables auditing of granting or revoking rights to users or groups, and establishing or breaking trust relationships with other domains.	Select Success Select Failure	Select Success Select Failure	Do not select	Do not select	Do not select	Do not select
File and Object Access	Enables the ability to turn on the auditing of access to a directory or file that is set for auditing.	Select Failure	Select Failure	Select Failure	Select Success Select Failure	Do not select	Do not select
Restart, Shutdown, and System	Enables auditing of shutdowns select and restarts of the computer, the filling of the Audit Log, and the discarding of audit entries if the Audit Log is already full.	Select Success Select Failure	Do not select				
Process Tracking	Enables auditing of the starting and stopping processes.	Do not select	Do not select				

For a domain controller, the Audit Policy window would look like this:



* Since the audit events are written to the event log, it is important to ensure that the Event Viewer, Event Log Settings are set such that data gathered will read before being overwritten.

Now that auditing has been enabled, it is very important to monitor the event logs frequently. If audit alerts go undetected, then hackers can continue penetrating your network. If your network has numerous systems that require monitoring, an intrusion detection system such as CyberSafe's Centrax (www.cybersafe.com) would be helpful.

Step 5:

Control Null Session Access:

Background Information:

A null session is created when a user logs on to an NT host using null username and null password. These sessions are considered to belong to the everyone and network group. Null sessions are mainly used for administrative purposes.

Risks:

Null sessions, although limited, allow access to some resources which can help an attacker to gain access to your network. After connecting to a resource using the null session, it may be possible to run the net view command to see all shares running on a remote system, the nbstat command to list ports, and other utilities.

Implementation:

It is possible to control null session access, but doing so may impact built-in utilities and applications that may use them. Trial and error may be the best way to determine which null session access can be locked out.

To Disable Null Session Access to Shares

1. In the registry, go to:
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanServer\Parameters
2. Create a new DWORD Value named: RestrictNullSessAccess
3. Set the value to 1.

To Disable Null Session Access to Named Pipes

1. In the registry, go to:
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanServer\Parameters
2. Modify the NullSessionPipes value – Remove named pipes from this list to block anonymous access (*Keep in mind that some applications may require null session access to named pipes).

© SANS Institute 2000 - 2002, Author retains full rights.

References:

Fossen, Jason and Kolde, Jennifer. *Securing Windows NT, Step-by-Step*. The SANS Institute: Network Security 2000.

McClure, Stuart and Scambray, Joel. *Hacking Exposed: Network Security Secrets and Solutions*. Osborne / McGraw-Hill 1999.

Brenton, Chris. *Mastering Network Security*. Sybex, Inc. 1998.

Fisch, Eric and White, Gregory B. *Secure Computers and Networks: Analysis, Design, and Implementation*. CRC Press, CRC Press LLC. 1999

“Securing NT” and “The Crux of NT Security - Phase One: The Approach”. SecurityFocus.com articles.

“Windows NT 4.0 Member Server Configuration Checklist”. Microsoft Technet document: mbrsrvcl.asp.

SANS student: Heckendorn, Sherri. Practical: Developments in Auditing NT. Incorporated Service Pack Research and added additional tool: Service Pack Manager by Gravity Storm Software. Added additional tips for enumerating all machines and domain controllers.

SANS student: McDowall, Tracey. Practical: Developments in Auditing NT: Information Technology Incorporated Password Policy Research and added additional password filtering tool: *Quakenbush Password Padlock*