Global Information Assurance Certification Paper

Organization: **The Fictitious Organization**
Network: **Fictitious Network**
Network Administrator: **System Administrator**
Auditor: **George Stanton**
Audit Date: **1/16/05**

Author: George Stanton
Date: Sunday, January 16, 2005

Purpose of this Document

This document was written to fulfill the practical requirements for GIAC certification in Securing Windows NT. The network described in this document is purely fictional. The intent is to provide a template by which to secure a small network with basic standard security. It is in no way intended to cover all aspects of securing networks under every set of circumstances.

Introduction

The Client has installed a startup Windows NT Network using the default install settings. Users on the network are connected to the Internet. The newly appointed Director of Information Technology has requested that a risk assessment and security audit be done.

Project Overview

Today it is all too common to associate a secured Internet connection with a secured network. To use an analogy this is like locking the front door of your home and leaving the back door and windows open while you go on vacation. Just like your home, there are many potential points of entry on the network and the entire network should be audited for potential vulnerabilities.

Phase I
Determine the Environment

Inspection of the work site and interviews with the system administrator and key personnel revealed the following.

- The network consists of a Windows NT4.0 Primary Domain Controller Server with about than 50 network client workstations on the network.
- All users have outbound access to the Internet for accessing the web and POP email accounts administered by an Internet Service Provider.
- There are future plans to host a company web site on premises.
- The network is entirely contained within the same building.
- The server is physically located on the floor in an unsecured room that doubles as an assembly and staging area for computer hardware. The entire work area is secured after business hours.

Organization:	**The Fictitious Organization**
Network:	**Fictitious Network**
Network Administrator:	**System Administrator**
Auditor:	**George Stanton**
Audit Date:	**1/16/05**

- There are several employees who are "Road Warriors" spending 80% of their time traveling. They all have modems attached to their desktop PCs for the purpose of accessing their network email and files stored on the network.

Define The Risk

The nature of risk to the information system is the maintenance of data integrity, the uninterrupted availability of the network, and the protection of information that is confidential and could be of value to business competitors. There are no current or planned Internet e-Commerce transactions taking place. Therefore standard settings and controls for a medium security network should be sufficient.

Define Project Goals

The objectives of this project are to:

1. Assess the current points of access to the Windows NT network; identify vulnerabilities and their possible exploitations.
2. With the assistance of the network administrator, perform an audit of current security controls and configure NT 4.0 servers to optimize network security.
3. Make recommendations on securing NT that will be included in the companies written "Stated Policies".
4. Identify vulnerabilities in the network that are not related to Windows NT but should be addressed in addition to securing the Windows NT Domain Controller.

Phase II

Audit and Reconfigure Windows NT4.0 Server Security.

Task 1 – Determine that the latest service pack has been applied.

Reason: As intruders find new ways to exploit Windows NT, Microsoft bundles fixes for security holes (especially DOS attacks) in service packs. Service Packs also may contain other important security features.

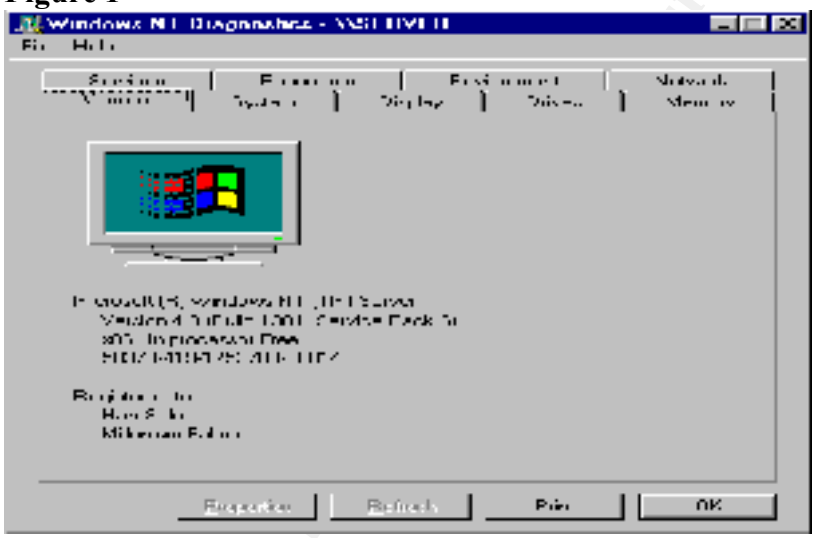
Recommendation: Always keep current with service packs. They are your cheapest and second most effective form of security. Unfortunately, developers testing service packs spend little testing time. Therefore, it is recommended that service packs be tested on a non-production server before distributing on the network. Latest service packs can be found at:
http://www.microsoft.com/ntserver/nts/downloads/default.asp#RecommendedUpdates

Organization:	**The Fictitious Organization**
Network:	**Fictitious Network**
Network Administrator:	**System Administrator**
Auditor:	**George Stanton**
Audit Date:	**1/16/05**

Performing Task I: To determine what service pack has been applied, click on the Start menu and navigate to Programs, Administrative Tools, and open Windows NT Diagnostics. With Windows NT Diagnostics you can access the local computer or browse to any computer to which you can connect. Clicking on the Version tab will display the service pack installed as seen in figure 1. The shortfall with this method is that it won't show any interim patches such as 6a. To see the exact service pack version and revision click Start, Run, and type winver. Then click OK. Note in figure 2 that the exact version (6a) is displayed.

It is also important to verify that the 128-bit encryption version of the latest patch was installed. You can verify this by looking in hive HKEY_LOCAL_MACHINE under SOFTWARE\Microsoft\Active Setup\Installed Components\ for the 128PATCH key. (See figure 3.)

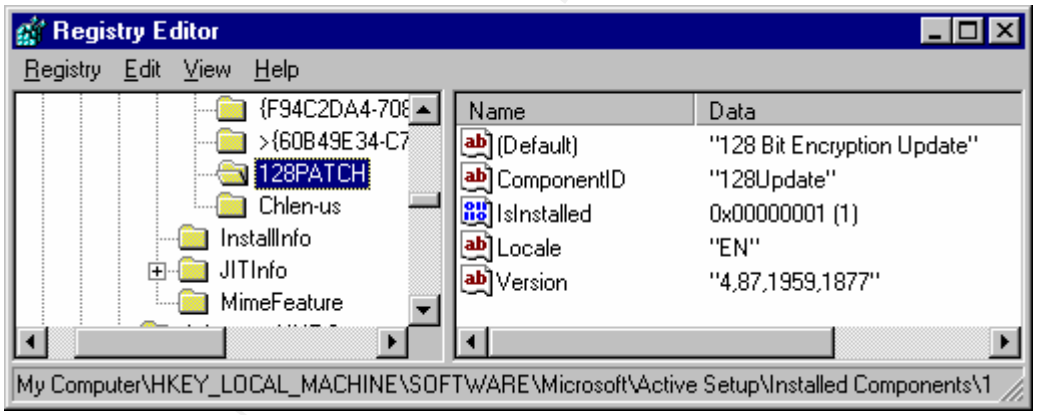
Figure 1



Organization:	**The Fictitious Organization**
Network:	**Fictitious Network**
Network Administrator:	**System Administrator**
Auditor:	**George Stanton**
Audit Date:	**1/16/05**

Figure 2

Figure 3



Task 2 – Disable the Messenger Service.

Reason: Messenger service is not necessary and can expose network information to intruders using the nbstat utility. Removing it reduces potential exposure.

Recommendation: Research Microsoft Knowledgebase documents for other nonessential services that may be stopped on your system. Unfortunately, this may require the trial and error method.

Perform task 2: Open Control Panel and then Services Note in figure 4 that Messenger service is running and was started automatically. Highlight the Messenger service, click

on Startup and change Startup Type to disabled as in figure 5. Click OK to return to services. Then manually stop the Messenger service. The next time you reboot the server the Messenger service will not start because you have it has been disabled.

Figure 4

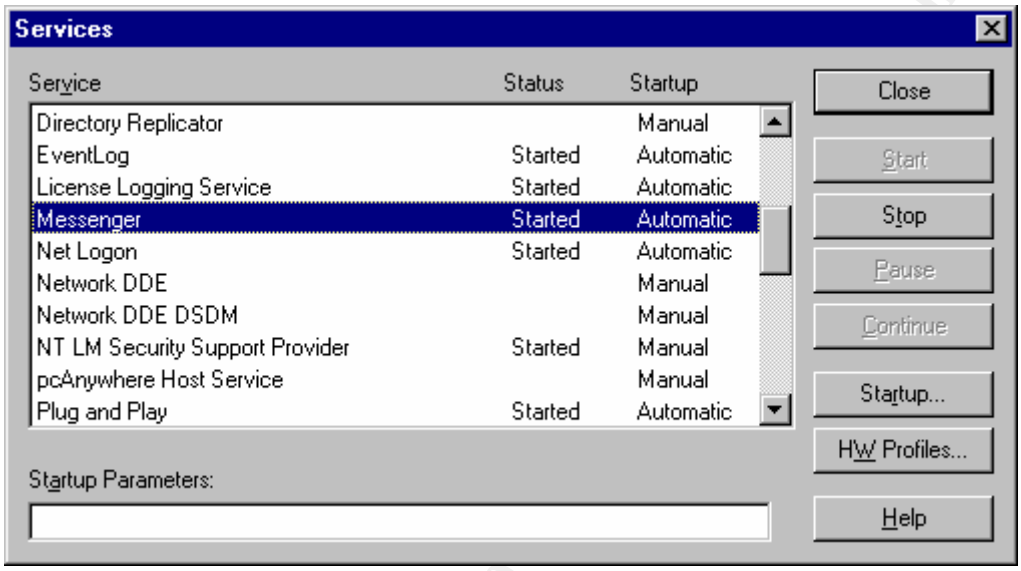


Figure 5

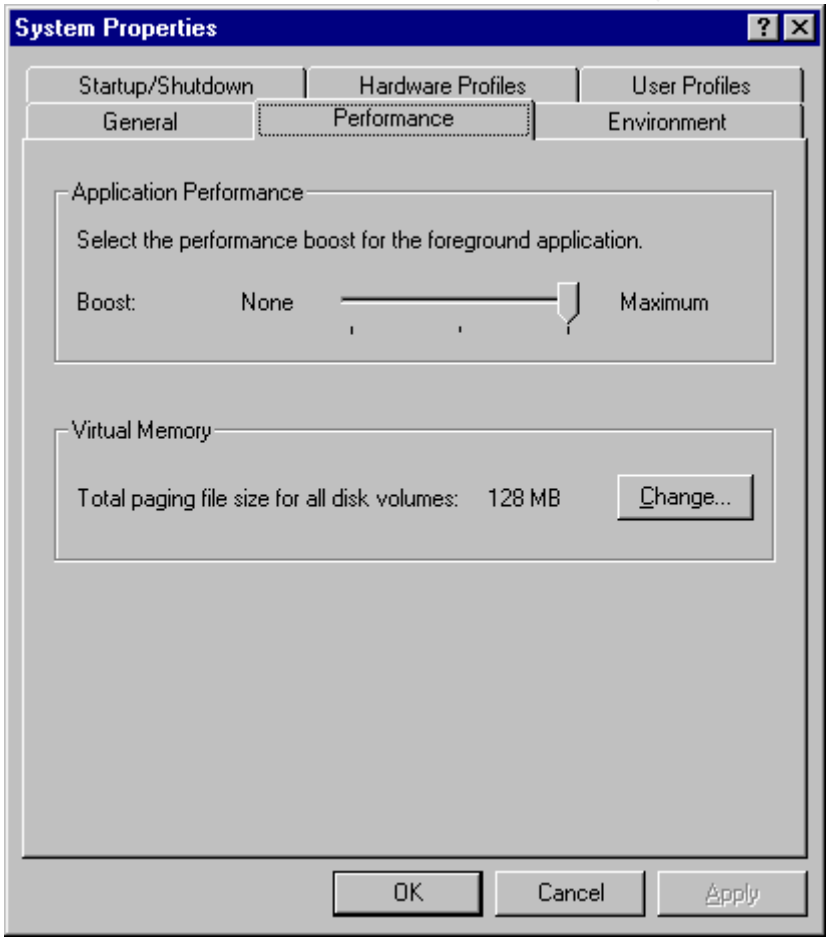
Organization:	**The Fictitious Organization**
Network:	**Fictitious Network**
Network Administrator:	**System Administrator**
Auditor:	**George Stanton**
Audit Date:	**1/16/05**

Task 3 – Preserve Ample Free Space For Temporary And Paging Files.

Reason: If Windows NT runs out of free hard drive space for temporary or paging files, whether in the course of normal activity or a DOS attack, the operating system may crash.

Perform task 3: From the Control Panel, open the System Properties. Click on the Performance tab. Note in figure 6 that the server has a total paging size of 128MB. The recommended paging size is equal to the size of RAM + 11MB. If you click on Change you can see in figure 7 that windows recommends 139MB for this server. For performance purposes the paging file will be moved to drive D, away from the operating system. This is done by highlighting the drive, entering the file sizes and clicking Set (see figure 8). The paging file is removed from the C drive by setting the values to 0 and clicking set. **Note:** the system will not be able to write crash dump files in the event of a STOP error unless there is a paging file on the same partition as the operating system.

Figure 6



Organization:	**The Fictitious Organization**
Network:	**Fictitious Network**
Network Administrator:	**System Administrator**
Auditor:	**George Stanton**
Audit Date:	**1/16/05**

Figure 7

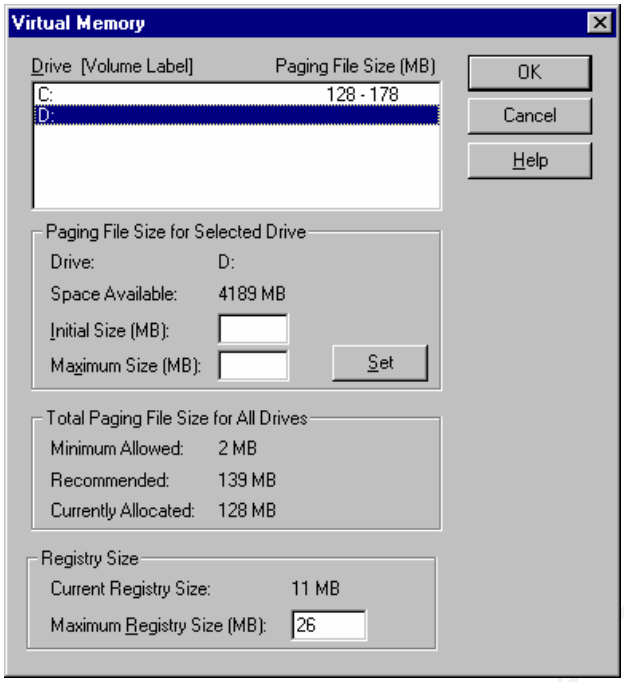
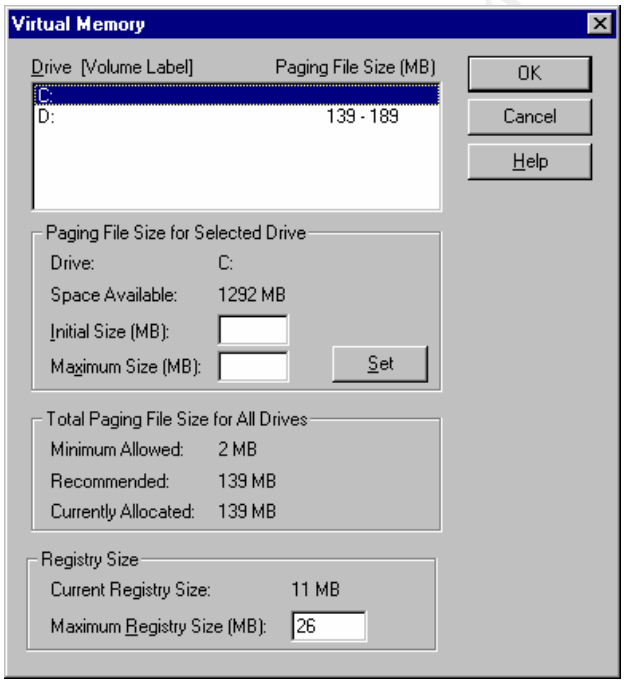


Figure 8



Organization: **The Fictitious Organization**
Network: **Fictitious Network**
Network Administrator: **System Administrator**
Auditor: **George Stanton**
Audit Date: **1/16/05**

Task 4 – Modify Registry To Mitigate (Not Eliminate) Potential Damage Caused By SYN Flood Attacks.

Reason: "SYN flood" is a common DOS attack that exploits the operating system by sending thousands of packets from a spoofed IP address with the SYN (synchronize) flag set on. The targeted machine replies at 3, 6, 12, 24, and 48-second intervals with a SYN-ACK response. In addition, during this 189 seconds of elapsed time, the target sets aside memory and CPU cycles to process the requests. When thousands of requests are sent in a short period of time, resources become overloaded constituting a DOS attack.

Perform task 4: Open the Start menu, run regedit, navigate to:

Hive: HKEY_LOCAL_MACHINE\SYSTEM
Key: \CurrentControlSet\Services\Tcpip\Parameters\
Add a new value named: SynAttackProtect
Value type: REG_DWORD
Set the value data to: "2" (See figure 9.)

Two (2) is the recommended setting for the following reason:
Options are 0, 1, or 2.

- 0 offers no protection (default).
- 1 reduces retransmissions of SYN-ACK retries.
- 2 is the same as 1 but additionally requires the completion of a three-way handshake before any additional resources are committed to the session.

Figure 9

Organization: **The Fictitious Organization**
Network: **Fictitious Network**
Network Administrator: **System Administrator**
Auditor: **George Stanton**
Audit Date: **1/16/05**

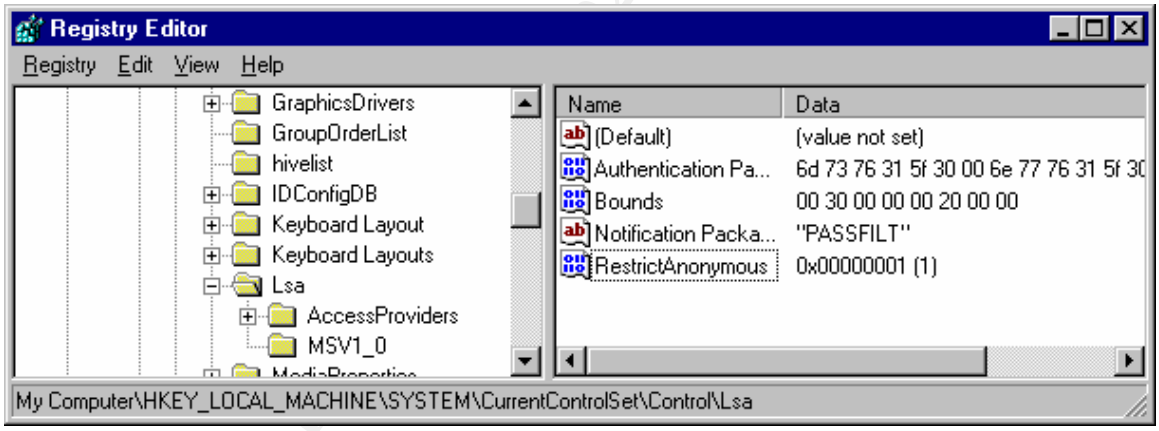
Task 5 – Block Null Sessions From Listing User Accounts.

Reason: Null sessions, by default can be used to list users from a remote computer. An intruder can exploit this. Since this network is a single domain there should be no adverse side effects of disabling this feature.

Perform task 5: Open regedit again and navigate as follows: (See figure 10.)

Hive: HKEY_LOCAL_MACHINE
Key: \SYSTEM\CurrentControlSet\Control\Lsa
Create the following entry:
Value Name: RestrictAnonymous
Value Type: REG_DWORD
Value Data: 1

Figure 10



Task 6 – Audit Password Policy and Secure the Password Database.

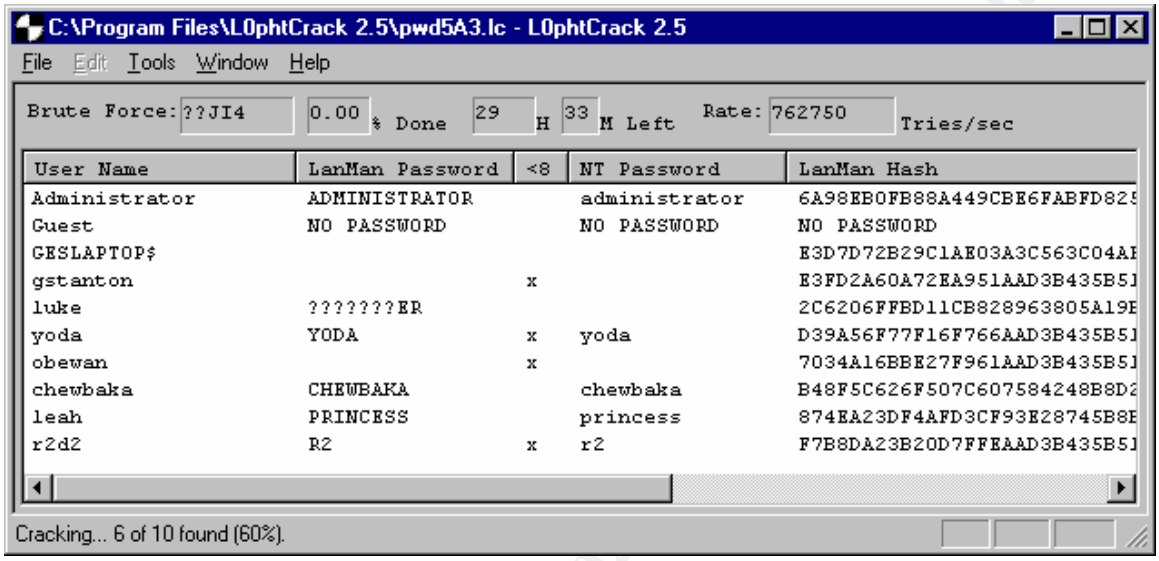
Reason: An intruder, interested in something more malicious than launching a DOS attack, will try to acquire a user account in order to steal, alter or destroy data.

Step 1: Run the L0phtCrack utility against the password hashes in the registry.

Results: Notice in figure 11, L0phtCrack cracked 60% of the passwords. Fifty percent were cracked just from the word list and one more was cracked one second into brute force. Also note that the Administrator is using administrator as it's password and the Guest user account has no password. Two additional users are using their username as their password.

Organization: **The Fictitious Organization**
Network: **Fictitious Network**
Network Administrator: **System Administrator**
Auditor: **George Stanton**
Audit Date: **1/16/05**

Figure 11

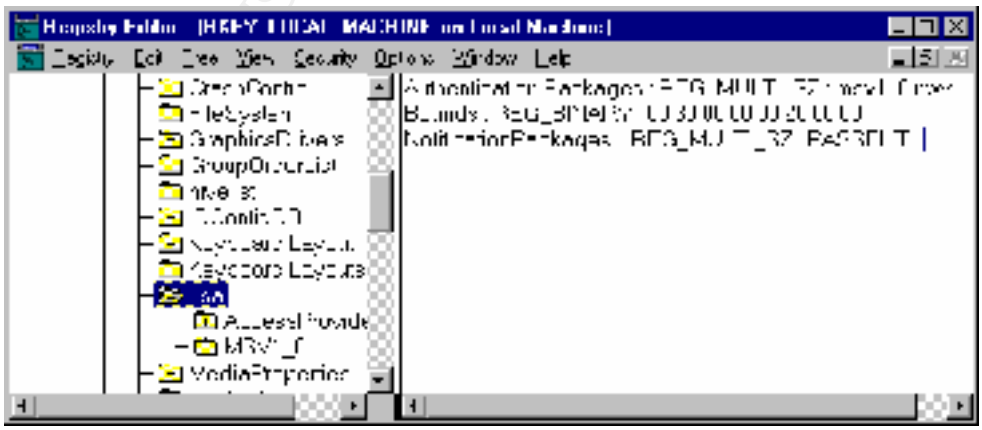


Recommendations: The following changes are to be made immediately.

Step 2: Filter out weak passwords by enabling passfilt.dll. The following addition to the registry will be made using regedt32 to enable password filtering: (See figure 12.)

Hive: HKEY_LOCAL_MACHINE
Key: \SYSTEM\CurrentControlSet\Control\Lsa
Value Name: NotificationPackages
Value Type: REG_MULTI_SZ
Value Data: PASSFILT

Figure 12



Passfilt will require that changed passwords be at least six characters long, not contain any part of the users full name and contain at least three of the four following categories of characters:

- Uppercase letters
- Lowercase letters
- Numbers
- Non-Alphanumeric symbols

Inform users about the new password policy. Open User Manager and set "User Must Change Password at Next Logon" by check marking the box next to the option.

Step 3: Create a "Honey Pot" Administrator account.

- Open User Manager. Rename the Administrator account and give it a password that uses a combination of all four of the character sets described above. Click the Policies, Rights tabs and remove Administrators from the "Access this computer from the network" rights group. Administrators can now only log on locally while sitting at the keyboard.

- Copy the newly renamed Administrator account (User, Copy from the User Manager Menu). Name the new account you create with the copy command "Administrator". Give this account a strong but guessable password. Remove all group membership rights. (A logon script will be written to alert the administrator if anyone logs into this account.) The administrator should log into this account frequently to give it the appearance of an active administrator account.

Step 4: Secure the Guest account.

- Open the Guest account, give it a non-blank password and disable the account. This prevents intruders from using the account to gain access. If there is a future need for a guest account, one can be created with a different name.

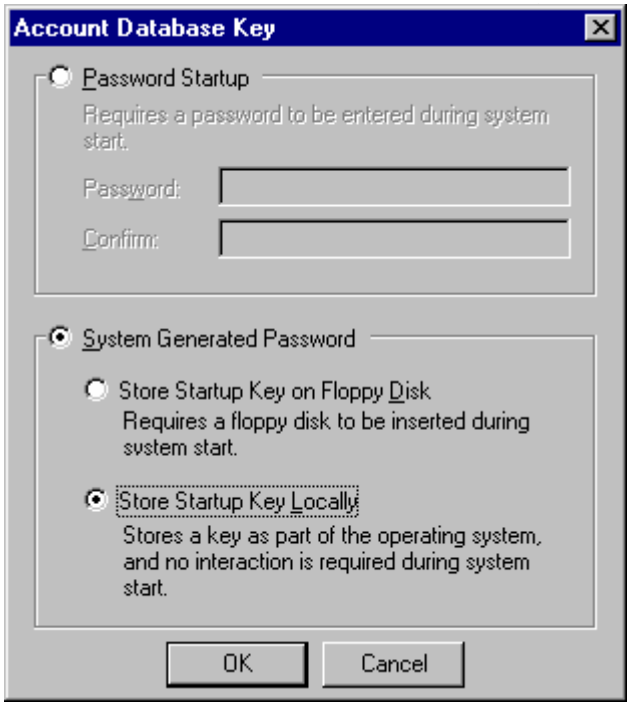
Step 5: Encrypt the SAM database. Before NTVLMv2 authentication can be enabled, all Windows NT4 clients must be verified as running SP4 or greater for compatibility. Until this can be accomplished we will encrypt the SAM database. Although this technique cannot prevent sniffing of over-the-network logon hashes, it does add a second layer of encryption by generating a 128-bit random key with which to encrypt the password hashes in SAM. This random key is then encrypted with a second key called the system key. For our current purposes we will store the system key on the local machine. This will protect the system from forgotten passwords and damaged boot diskette, either of which would render the system un-bootable.

- To encrypt the SAM database click Start, then click Run. Type syskey and click OK. At the window titled "Securing the Windows NT Account Database", select

Encryption Enabled and then click OK. (See figure 13.) On the Account Database Key screen select System Generated Password and Store Startup Key Locally. Click on OK. (See figure 14.)

Figure 13

Figure 14



Organization:	**The Fictitious Organization**
Network:	**Fictitious Network**
Network Administrator:	**System Administrator**
Auditor:	**George Stanton**
Audit Date:	**1/16/05**

Task 6: Secure NetLogon Channels.

Reason: When a Windows NT machine joins a domain a machine account is created which is used on boot up to create a secure channel to the domain controller. Requests sent on this secure channel are authenticated and passwords are encrypted. However, there is still a risk of possible packet sniffing followed by a man-in–the-middle attack.

According to Microsoft Knowledgebase Article Q183859, "Lack of integrity checking means that it is possible for an attacker who can intercept and modify requests to modify information in requests or responses undetected. Use of such an attack to modify group membership information could allow an attacker who has interactive logon access to a workstation to become administrator on that workstation."

Recommendation: Service pack 4 introduced the capability of greatly increasing NetLogon security by requiring integrity checking and/or encryption. The following Registry values can be used to modify the behavior of the secure channel between the client and domain controller. All of the following values can be set in the registry under the following key:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\netlogon\parameters
```

The following are the possible settings. All are
Value Type: REG_DWORD - Boolean
Valid Range: 0 (FALSE) or 1 (TRUE)

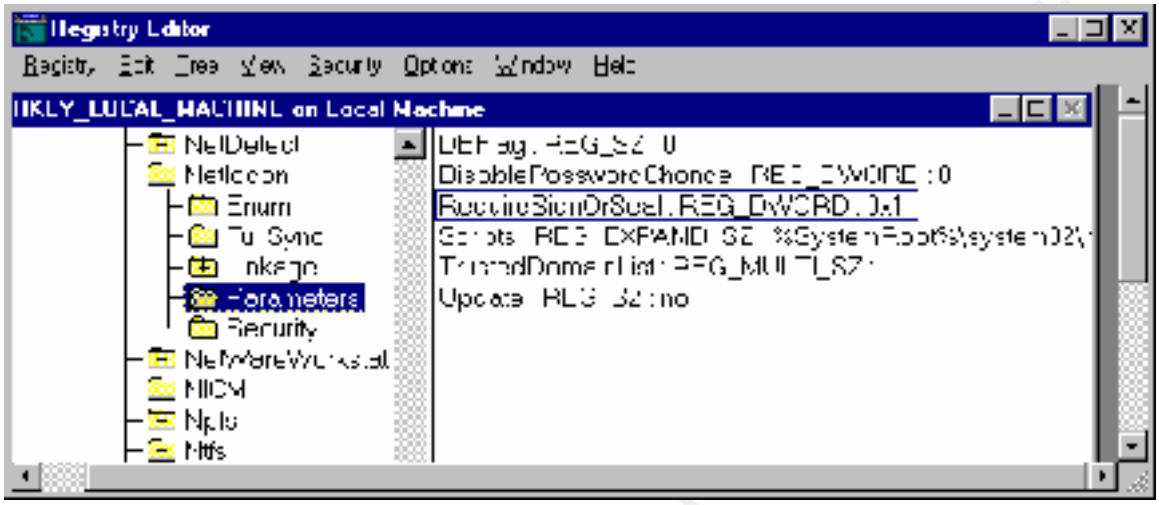
SignSecureChannel: This parameter specifies that all outgoing secure channel traffic should be signed. If SealSecureChannel is also TRUE, it will override any setting for this parameter and force it to TRUE.

SealSecureChannel: This parameter specifies that all outgoing secure channel traffic should be encrypted.

RequireSignOrSeal: **(See figure 15)** This parameter specifies that all outgoing secure channel traffic must be either signed or sealed. Without this parameter, this is negotiated with the Domain Controller. This flag should only be set if ALL of the domain controllers in ALL the trusted domains support signing and sealing. If this parameter is TRUE, SignSecureChannel is implied to be TRUE.

Organization:	**The Fictitious Organization**
Network:	**Fictitious Network**
Network Administrator:	**System Administrator**
Auditor:	**George Stanton**
Audit Date:	**1/16/05**

Figure 15



Task 7 Control Access To Network Resources.

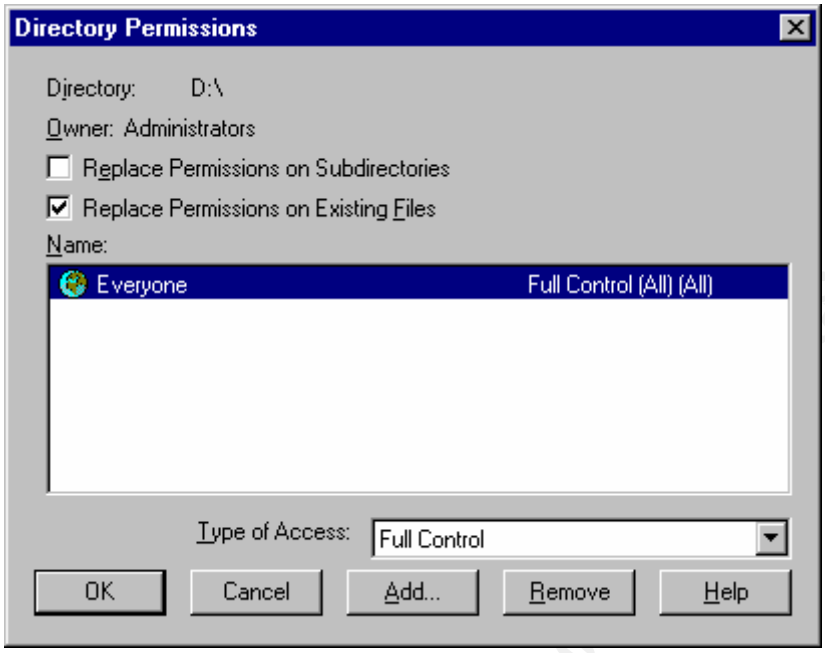
Reason: Once an intruder acquires a user account the intruder can perform in depth reconnaissance under the cloak of a legitimate user as well as gain direct access to any resources the user has rights to. Statistically most intruders already have a legitimate account. This is because, according to the FBI "Employees commit most of the reported crimes."

Perform task 7:

Step1: Remove the group Everyone from NTFS Security Permissions. This group contains literally everyone who logs on and by default is granted full control to NTFS volumes. Open Administrative Tools, Disk Administrator. Highlight NTFS volumes. Select Tools, Properties, Security, Permissions. You will see a window like figure 16. Remove the Everyone group from the permission list.

Organization:	**The Fictitious Organization**
Network:	**Fictitious Network**
Network Administrator:	**System Administrator**
Auditor:	**George Stanton**
Audit Date:	**1/16/05**

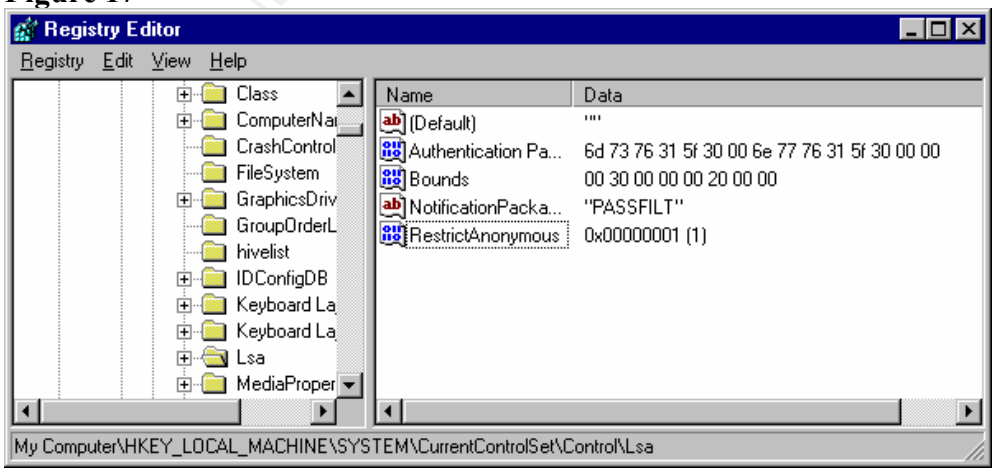
Figure 16



Step 2: Block Null Users From Listing Share Names. Add the following registry value. This is actually controlled by the same RestrictAnonymous value that was applied in task 5 so it has already been done. This step was included for documentation purposes. (See figure 17.)

Hive: HKEY_LOCAL_MACHINE
Key: \SYSTEM\CurrentControlSet\Control\Lsa
Value Name: RestrictAnonymous
Value Type: REG_DWORD
Value Data: 1

Figure 17



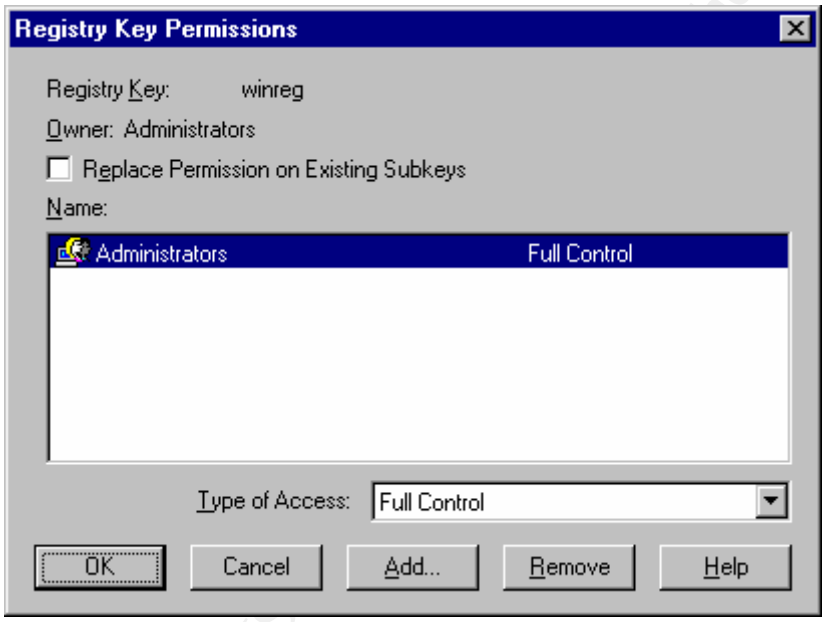
Organization:	**The Fictitious Organization**
Network:	**Fictitious Network**
Network Administrator:	**System Administrator**
Auditor:	**George Stanton**
Audit Date:	**1/16/05**

Step 3: Control Network Access To The Registry. The registry editor can be used to access the registries of remote machines on the network. To control access, edit the permissions to the following key:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg

To modify permissions you must use regedt32(not regedit). Navigate to the winreg key in the above path. Click the security tab and select permissions. You will see a window like figure 18. Removing all users from the security grants will prevent anyone from remotely accessing the registry.

Figure 18



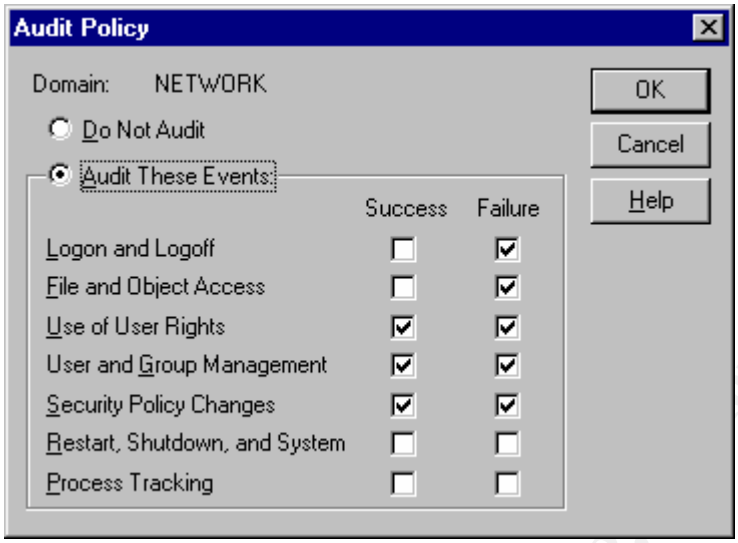
Task 8: Enable Auditing.

Reason: Windows NT, although it includes extensive auditing capabilities, audits nothing by default. Event auditing is the most important step you can take to detect intruders. Minimal logging, at the very least, should be enabled.

Perform task 8: Auditing is set up in the User Manager by clicking on the Policies, Audit tab in the program menu and check marking the events to be audited. We will begin by auditing the following events as check marked in figure 19.

Organization:	**The Fictitious Organization**
Network:	**Fictitious Network**
Network Administrator:	**System Administrator**
Auditor:	**George Stanton**
Audit Date:	**1/16/05**

Figure 19



Configure the Security Log. The security log file has to be large enough to hold the events written to it. The size of the log depends on the amount of data that will be written to it over a period of time, so it may require trial and error. Setting a large maximum file size does not pre-allocate that amount of space on a drive. So we'll set it large for now. We'll also set the log file to wrap every 11 days. This gives us plenty of redundancy with a weekly backup plan in place. (See figure 20.)

Figure 20

Organization:	**The Fictitious Organization**
Network:	**Fictitious Network**
Network Administrator:	**System Administrator**
Auditor:	**George Stanton**
Audit Date:	**1/16/05**

Task 9: Create An Updated Emergency Repair Disk

Reason: After making changes to the registry it is important to create an updated Emergency Repair Disk so that if you must repair your system it will reflect it's current state.

Perform Task 9: Click Start, Run, and type Rdisk.exe and OK. Select Update Repair Info.

Phase III
Summary and Recommendations

Domain Controller

The Windows NT Primary Domain Controller has been audited for vulnerabilities and configured for a standard level of security. There may be further control settings that the system administrator may wish to adjust after further auditing and evaluation of the benefits and consequences. Further information on Microsoft NT Domain Controller Security settings can be obtained at http://www.microsoft.com/technet/security/dccklst.asp.

System Administrator

1. The system administrator needs to set aside time to review security logs regularly or explore the possibility of purchasing an automated event log analyzer.
2. The system administrator should receive formal security training from SANS Institute or other reputable source.
3. The system administrator should keep abreast of the latest security developments by checking www.sans.org and other pertinent security sites.

Firewall – Implement one ASAP - This will be first line defense against intrusion from outside your network.

Physical Security: Physical security is most often overlooked. Statistics prove that most damage caused to networks comes from internal sources.

1. The Server room should be equipped with a lock system and secured from any access by persons other than authorized IT staff.
2. The Servers and other equipment should be raised off the floor in CPU racks or computer tables.
3. The Sprinkler system in the computer room should be disconnected or some method devised to protect the equipment from being soaked.

4. Backup tapes and emergency repair disks should be stored in a secure location. Giving a potential attacker access to Emergency Repair Disks is like leaving the keys in your car.
5. A dial in remote access server should be installed in the computer room with a modem pool for "road warriors" to dial into. Modems should be removed from all user computers. Phone lines that are installed for these modems should be assigned non consecutive numbers that are out of the range of the companies voice numbers (preferably with a different prefix).
6. All users should be taught to lock their workstations when leaving them. Use of screensavers with passwords should be enforced.

Social Engineering Awareness: A clever or charming attacker can enlist the help of unsuspecting, well-meaning employees. Help desk staff should be educated about social engineering. A policy should be developed to control any changes of passwords or privileges, especially via the telephone.

References

Fossen, Jason and Kolde, Jennifer. SANS institute GIAC Training 2000.

SANS Institute. "Securing Windows NT: Step-by-Step, Parts 1,2 & 3", 2000 .

Microsoft Knowledge Base. http://support.microsoft.com/directory/default.asp.

Microsoft TechNet http://www.microsoft.com/technet.

Garms, Jason. Windows NT Server 4 Unleashed, Sams Publishing..

SANS Institute Security Digest. http://www.sans.org/digests/ntdigest.htm

Last Updated: July 27th, 2017

Upcoming Training

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