Global Information Assurance Certification Paper

Martin A. Golias
246 Airport Road
Johnstown, PA 15904

Phone 814-534-8879
Practical T1 Track Parliament Hill, Ottawa

The purpose of this paper is to demonstrate practical methods to secure file servers and company services. It is in not meant to be a complete or final set of rules or procedures in that network security is an ever developing set of techniques of hackers and network administrators.

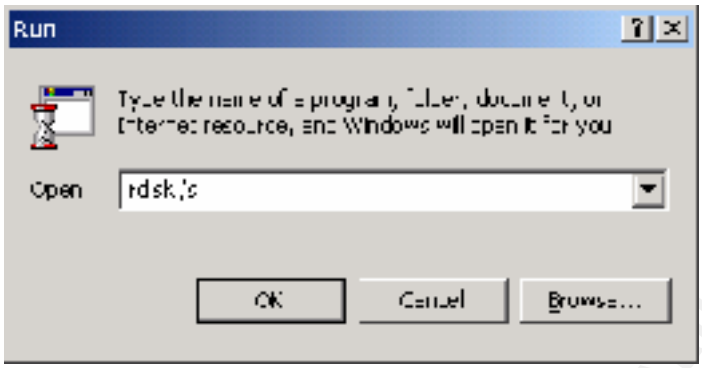
I plan on using some of the techniques learned at the SANS Parliament Hill classes and additional information acquired from the Internet and in particular Microsoft to demonstrate a working knowledge of steps necessary to implement and research security techniques.

Outline of practical demonstrations

Section 1
Prepare for recovery: Emergency repair disks

The ability to recover from a hacker exploit or other disaster is essential. While tape backups are critical not all of them can save/restore the boot sector and the Master Boot Record. It is essential that a set of Emergency repair disks be prepared, updated frequently and stored in a safe place.

From the Run line execute the following command.



The system will save the current configuration
Next you will be asked if your want to create the Emergency Repair Disk. Click on Yes.
The floppy that you are using will be formatted. Click on OK.
You are then instructed to store the ERD in a safe place. Click on OK.

The command above contains the /s switch in order to have a current copy of the SAM database. Without the /s switch only the administrator and guest account OF THE ORIGINAL INSTALLATION are copied to the ERD.

In addition to the ERD disk created for each file server the following disks are also necessary.

An Emergency NT Boot Disk

Three bootable setup disks with a current copy of Setupdd.sys on the second disk if your file server is at Service Pack 6 or later.

Finally you should have a MS-DOS boot disk such as a Windows 98 emergency Boot Disk with utilities such as FDISK, FORMAT, Partition Magic and CD-ROM and tape drivers.

Reference: SANS Parliament Hill 2000 manual page 57.

Section 2
Limiting information accessible to anonymous users in Exchange

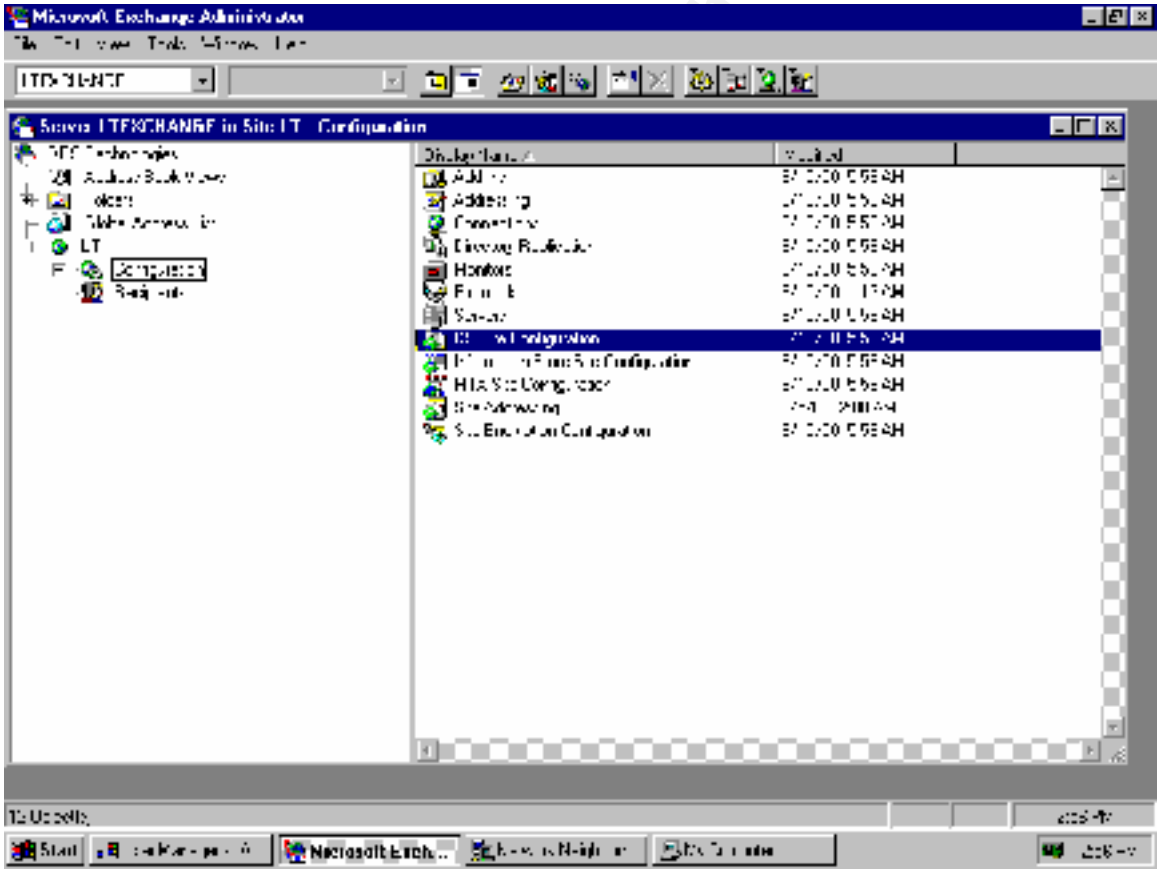
Microsoft Exchange, by default, allows anonymous users to search the Exchange Global Address List with an LDAP (The Lightweight Directory Access Protocol) client like Microsoft Outlook Express. Due the incredible amount of data that can be input into the exchange client, information can be acquired and used for social engineering to gain access to unauthorized information.

Steps in limiting the access of information to LDAP users is as follows:

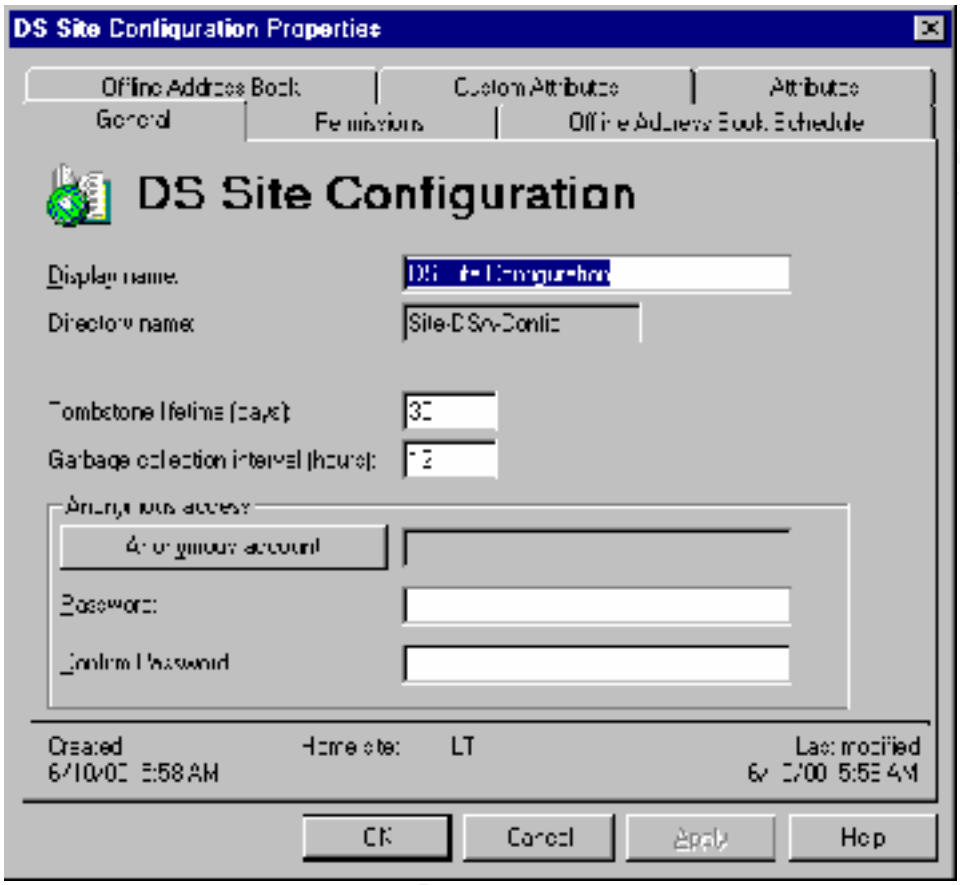
At the Exchange server launch the Microsoft Exchange Administrator.

Highlight Configuration on left panel.

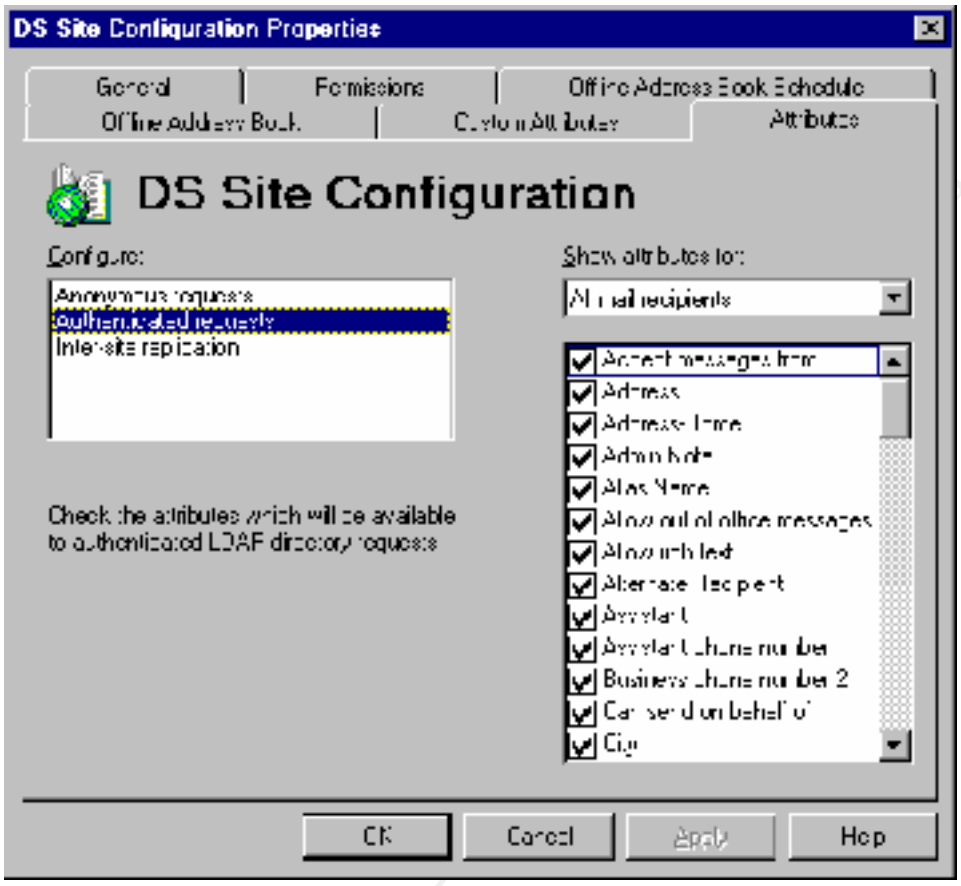
Double Click on DS Site Configuration on the right panel.



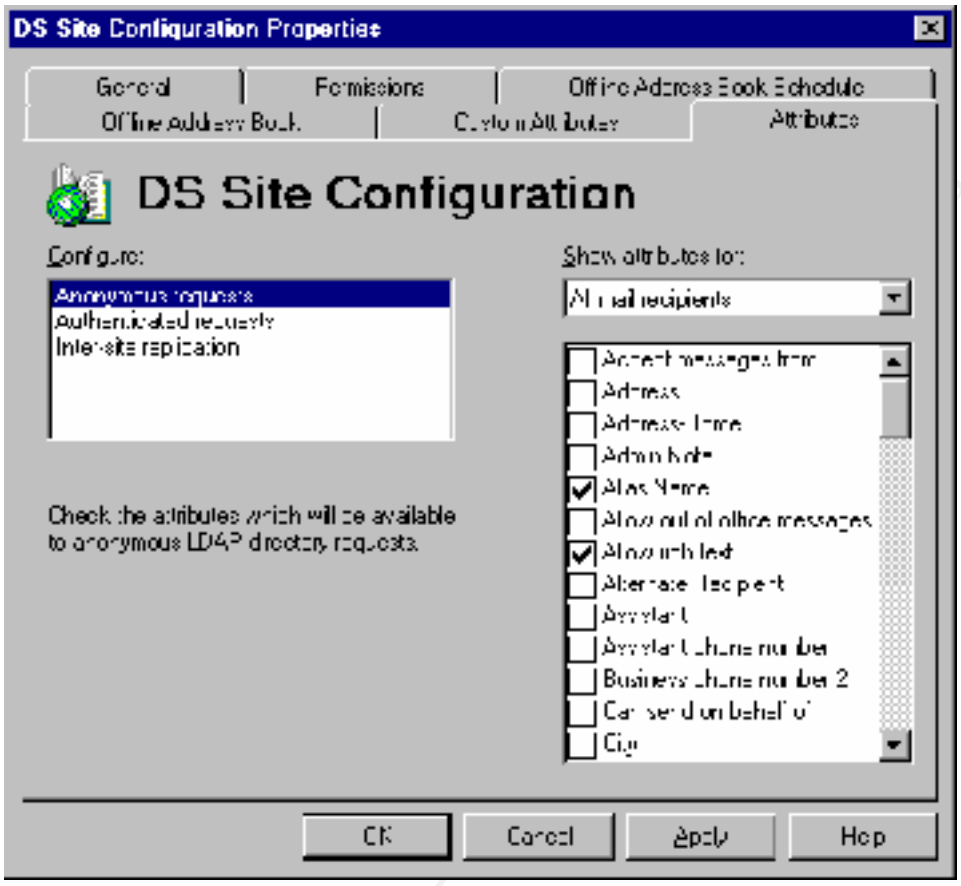
After clicking on the DS Site Configuration Properties screen, click on the Attributes Tab.



In the example that I am using, authenticated requests to the Exchange directory have the ability to view all of the attributes.



Then, with Anonymous requests highlighted, check or uncheck the information attributes that you want the anonymous user to be able to access.



In my example, I removed the ability of the LDAP users to view the users home phone number, address, first name, department, the persons manager, mobile phone number and any notes about the mail recipient and any other information that could allow an individual to be compromised by social engineering.

What is left would be the maximum I would want anonymous users to be able to view.

This same technique could be used to limit information for authenticated and to limit or augment Inter-site replication.

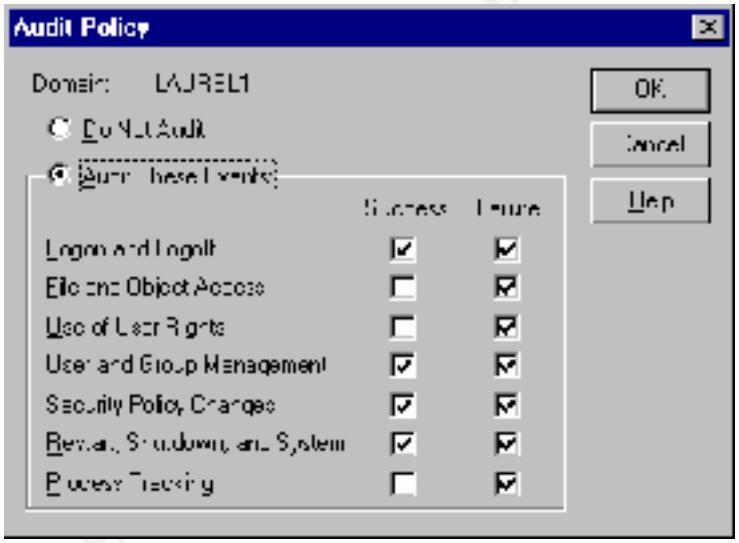
Reference: SANS Parliament Hill 2000 manual page 31.

Section 3
Security Event Auditing

NT Server maintains three event logs to which entries are added – the System log the Applications log and the Security log. You can set up security auditing of numerous events to assist in tracking users access to various parts of the system.

Proper setting and monitoring the Audit Logs created by the Audit Policy administrators can keep watch on unauthorized access to files.

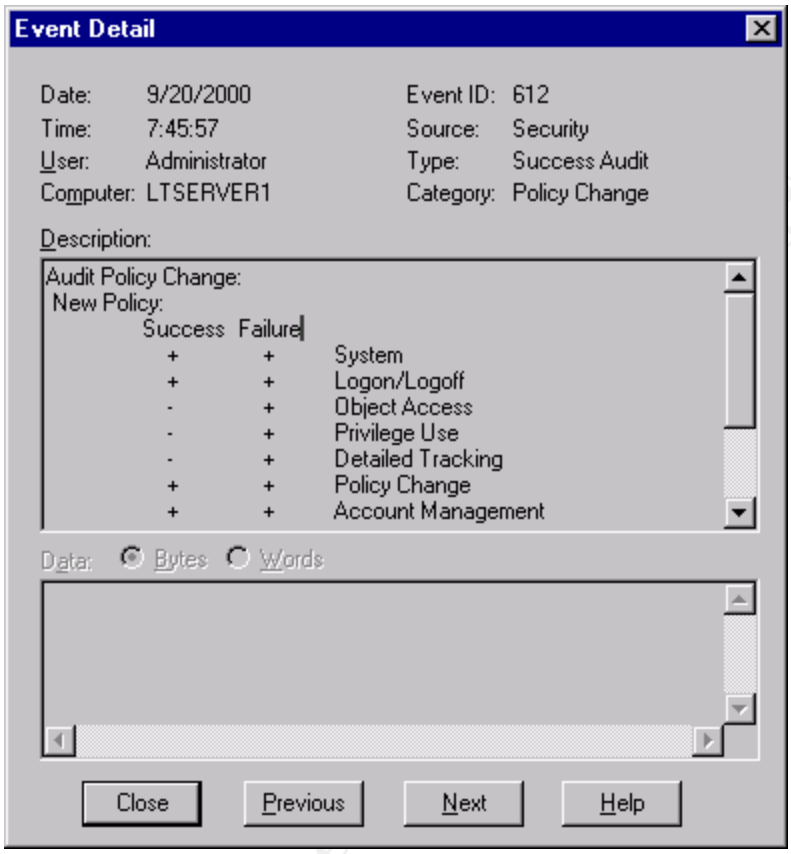
Steps in accomplishing this are as follows.
Click on User Manager for Domains
Highlight Policies
Click on Audit
NOTE: The default setting for auditing is Do Not Audit.



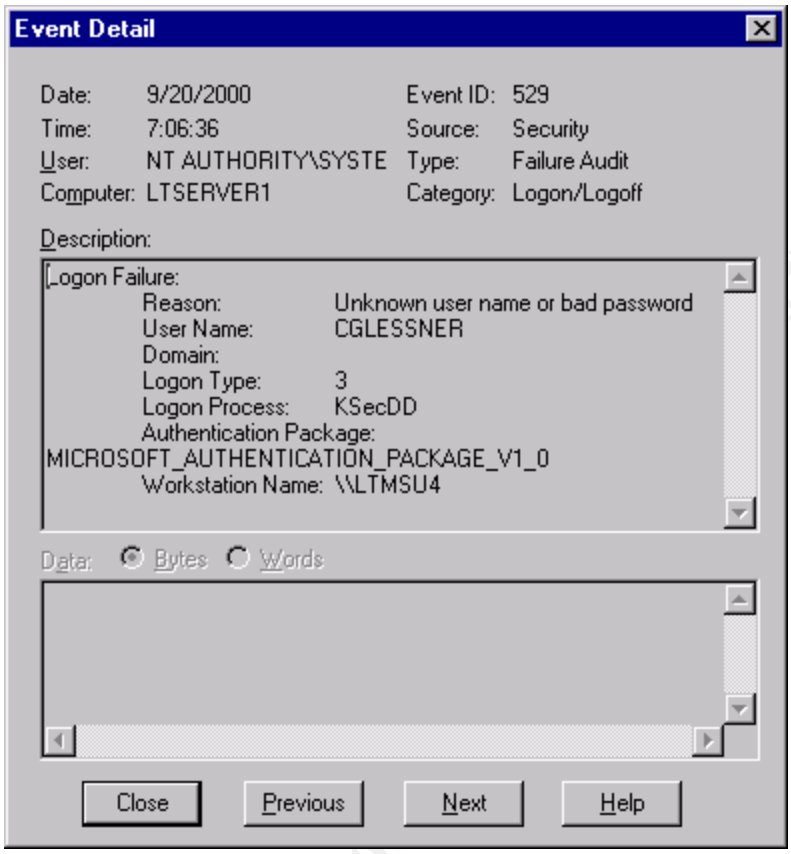
Once the events that you want to audit have been selected you can open the Event Viewer by going to:
Start
Programs
Administrative Tool (common)
Event Viewer
Then scroll to the event that you want to investigate and double click.

In my example I wanted to verify that the Policy Change that I had chosen was logged and that the system was auditing for login failures.

Event Detail for a successful Policy Change.



Event Detail for an unsuccessful login



Notes:

Because of the amount of logging required for my location I have increased the log file size from the default size of 512 KB for the Security log, System log and the Application log. Also, there is a small performance overhead factor for each audit check the system performs.

For auditing to be effective regular inspection of the logs is necessary.

Reference: Microsoft Windows NT Server Networking Guide.

Section 4
Verify latest service pack from Microsoft

Microsoft Service packs are a collection of upgrades and patches for Microsoft servers. Many of the upgrades or patches are developed to fix security holes in the Microsoft NOS.

1. For each domain controller:
    1. Click Start, click Run.

    2. Type "Winver" and press enter.

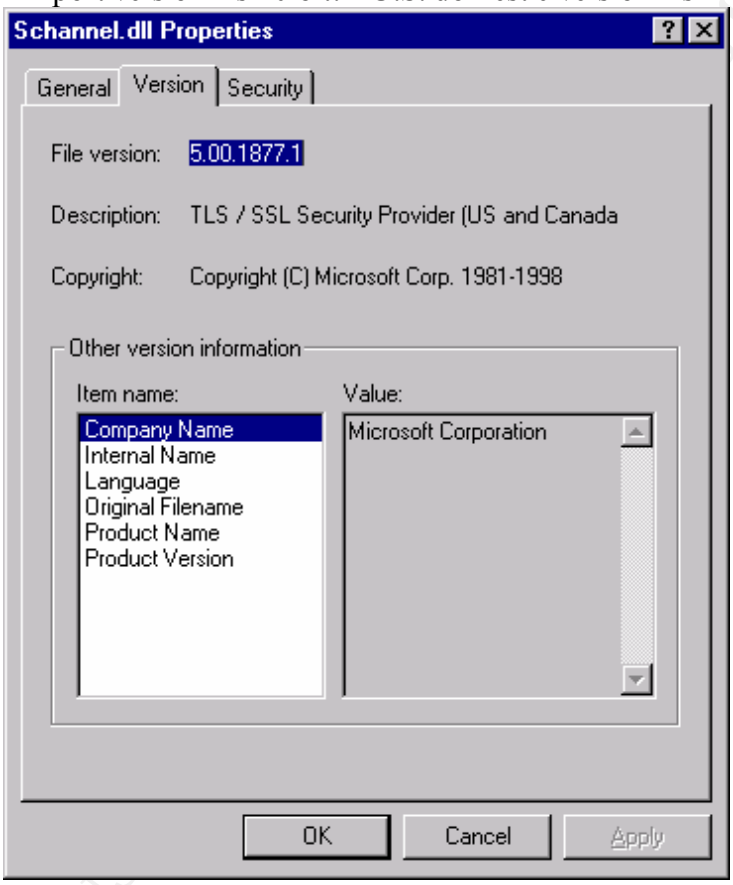
    3. Note the Service Pack installed: _Revised Service Pack 6a___.

4. Click Start, point to Programs, and then click Windows NT Explorer.

5. Click the Winnt folder and then click the System 32 folder.

6. Right click on Schannel.dll, click Properties, click version tab and then view description.

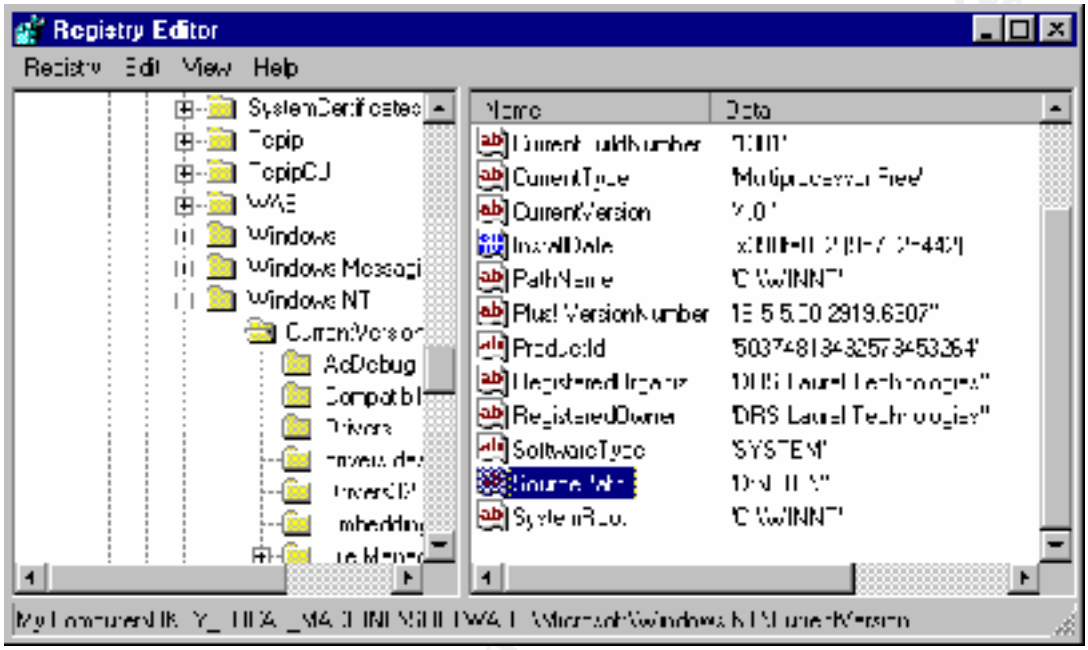
7. Note encryption level: __U.S. and Canada (128 bit)_
"Export version" is 40-bit. "U.S. domestic version" is 128-bit.



If these service packs were not up to the current version, access the Microsoft site and either download the entire service pack to keep on CD or do a live update. If you believe that there is a possibility of a root kit or other hacker materials it would be best to download the service pack in it's entirety and proceed with the service pack installation.

Finally, point the source path of the service pack updates to the update folder on the file server. This is to eliminate the re-application of the service pack each time that changes are made to the file server.

Hive: HKEY_LOCAL_MACHINE
Key: \Software\Microsoft\Windows NT\CurrentVersion
Value Name: SourcePath
Value Type: REG_SZ
Value Data: <path to the distribution NT files.



NOTE: The current service pack is NOT always recommended for a application specific server. The application ISS RealSecure is currently only tested and approved at Service Pack 5.

Reference: SANS Parliament Hill 2000 page 41.

Section 5
Tuning TCP Parameter for SYN floods

A common DOS attach is a SYN flood. The following is a brief description of what a SYN flood is a Denial of Service attack.

Technical Description: A standard TCP connection is established by sending a SYN packet to the destination host. If the destination is waiting for a connection on the specified port, it will respond with a SYN/ACK packet. The initial sender then replies to the SYN/ACK with an ACK packet, and the connection is established. When the SYN/ACK is sent back to the source, a block of memory is allocated to hold information about the state of the connection that is currently being established. Until the final ACK is received or a timeout is reached, this block of memory sits unused, waiting for more information to be received from the source host. By sending numerous SYN packets to a host, the destination will exhaust the portion of memory it has on-hand to deal with opening connections. Legitimate connections will no longer be able to connect to the host. The flood of SYN packets can detect this situation without accompanying responses. It can be corrected by sending the destination RST packets that correspond to the initial SYNs. This results in the destination host freeing up that block of memory and making room for a new legitimate connection.

Why this is important: Most systems have a pre-defined limit of active TCP connections. Once this limit is reached, additional connections are ignored. A SYN Flood attack attempts to use up these connections and then leave them idle so that the victim station cannot accept any additional connections.

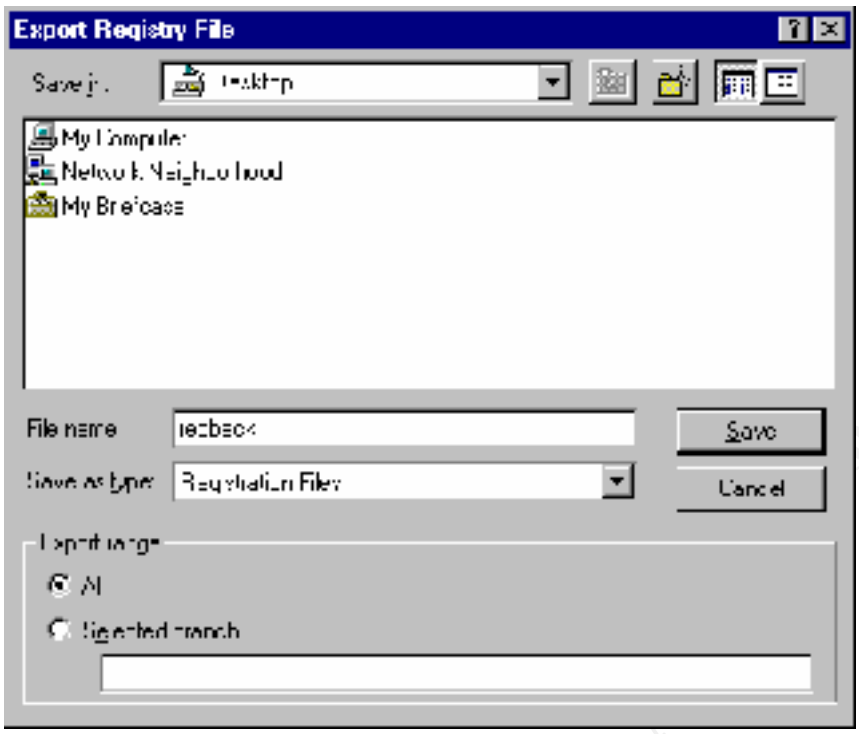
How to remove this vulnerability: You should consider upgrading your operating system version or applying a service patch. Many operating systems now have heuristics for terminating idle connections that prevent SYN Floods from locking out valid connections. You can also increase the default limit of connection buffers.

Available in Service Pack 5 and later is a registry value that can reduce the number of SYN-ACK retries.

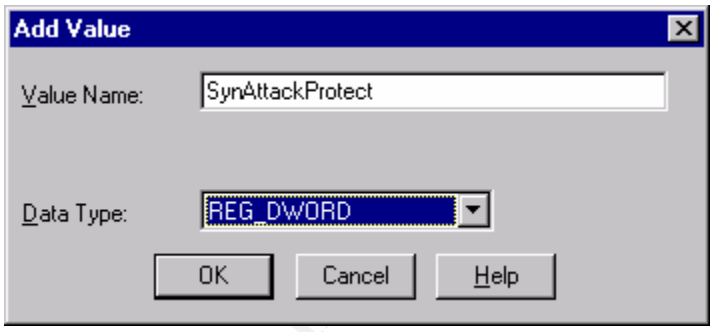
From the Run command line type REGEDIT and click on OK.

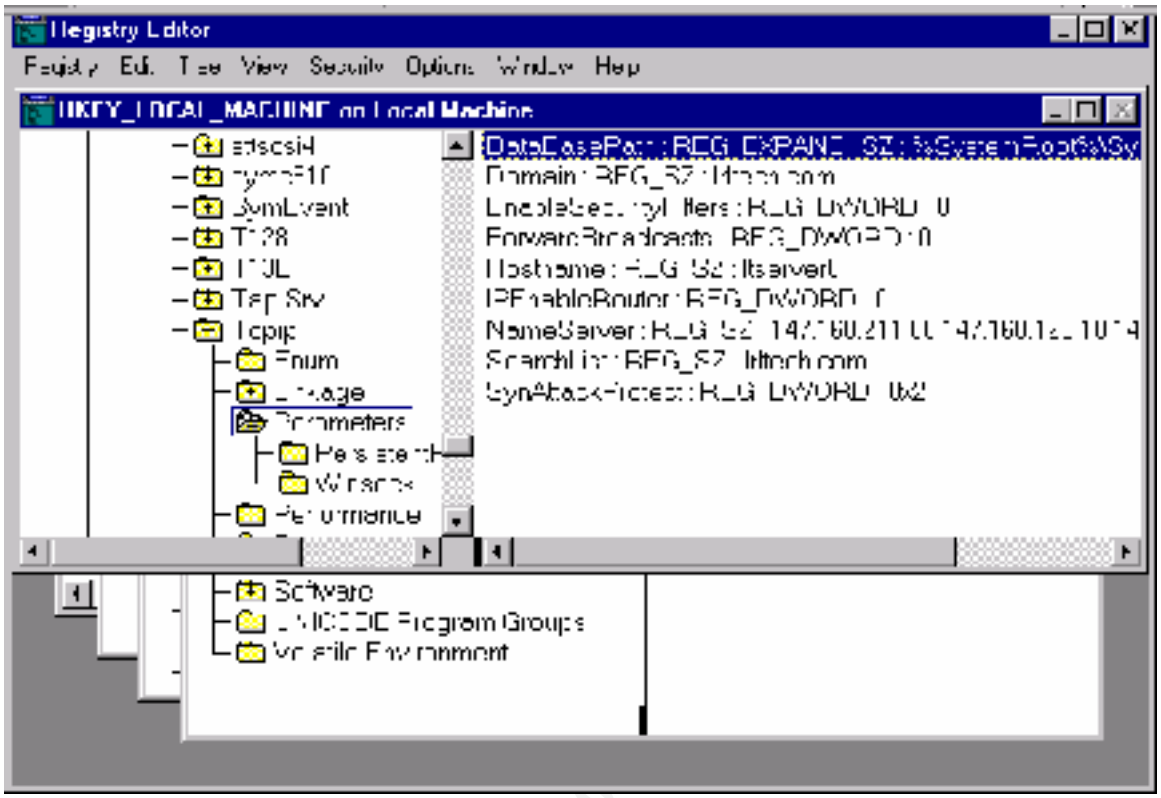
When editing the Registry it is always advisable to export a copy of the Registry before making any changes. This will enable you to restore the Registry if there are any problems with the additional or changed Registry value.

Make a backup of you current Registry.



Open REGEDT32 and make the following change to your registry.





Hive: HKEY_LOCAL_MACHINE
Key: \System\CurrentControlSet\Services\Tcpip\Parameters
Value Name: SynAttackProtect
Value Type: REG_DWORD
Value Data: 2

The Value Data of 2 reduces the AYN-ACK retries and also the full three-way handshake must complete before the afd.sys driver commits additional resources.

Reference:
SANS Parliament Hill 2000 page 54.
RealSecure on-line documentation.

Section 6
Setting Security Policies

User access to network resources – files, folders and devices – in NT Server is controlled in two ways: by assigning rights to a user that grant or deny access to certain objects and by assigning permissions to objects that specify who is allowed to use objects and under what conditions.

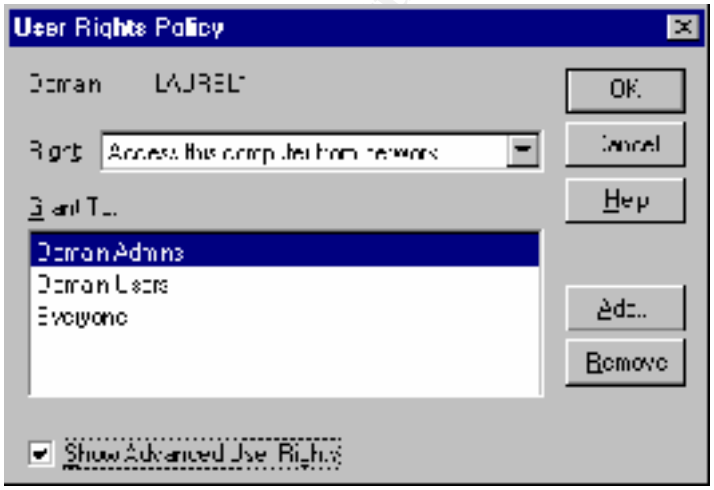
Rights generally authorize a user to perform certain system tasks such as logging on to a server, back up and restore data or modify printer options on a shared printer.

Proper setting of the User Rights Policy found in the User Manager for Domains is essential.

Properly setting the User Rights Policy can help in securing your network. If an intruder or a displaced network administrator can set up what is being audited and what user rights can be controlled the security of your network can be compromised.

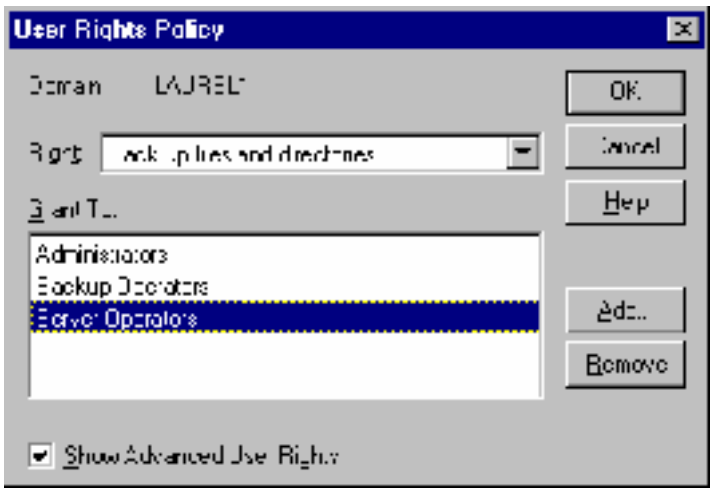
Steps in accomplishing this are as follows.

Click on User Manager for Domains
Highlight Policies
Click on User Rights
Check the box for Show Advanced User Rights.



After you have accessed the above screen click on the **Right:** drop box and choose the rights that you want to modify.

For this example, use the drop down box to choose **Back up files and directories.**



The rights that are granted to an individual or a group to back up files is very important because the backup operator must have access to all files in order to back them up.

As shown in the table below, from Microsoft, you only want **trusted** individuals or groups to be able to do this. Trusted groups for Domain: Lauel1 are Administrators, Backup Operators and Server Operators. If you want to Add or Remove users or groups double click on the appropriate box and choose the user/group that you want to add or remove.

User Right	Domain Controllers	Member Servers	Workstations
Access this computer from network	(anyone)	(anyone)	(anyone)
Act as part of the operating system	(no one)Do not assign to any user.	(no one)Do not assign to any user.	(no one)Do not assign to any user.
Add workstations to domain	(no one)	(no one)	(no one)
Back up files and directories	**trusted users**	**trusted users**	**trusted users**
Bypass traverse checking	(anyone)	(anyone)	(anyone)

Change the system time	trusted users	trusted users	trusted users
Create a pagefile	trusted users	trusted users	trusted users
Create a token object	(no one)Do not assign to any user.	(no one)Do not assign to any user.	(no one)Do not assign to any user.
Create permanent shared objects	(no one)	(no one)	(no one)
Debug programs	(no one)This right is not auditable and should not be assigned to any user, including system administrators.	(no one)This right is not auditable and should not be assigned to any user, including system administrators.	(no one)This right is not auditable and should not be assigned to any user, including system administrators.
Force shutdown from a remote system	trusted users	trusted users	trusted users
Generate security audits	(no one)Do not assign to any user.	(no one)Do not assign to any user.	(no one)Do not assign to any user.
Increase quotas	trusted users	trusted users	trusted users
Increase scheduling priority	trusted users	trusted users	trusted users
Load and unload device drivers	trusted users	trusted users	trusted users
Lock pages in memory	(no one)	(no one)	(no one)
Log on as a batch job	trusted users(as needed)	trusted users(as needed)	trusted users(as needed)
Log on as a	trusted users(as	trusted users(as	trusted users(as

service	needed)	needed)	needed)
Log on locally	trusted users	(anyone)	(anyone)
Manage auditing and security log	trusted users	trusted users	trusted users
Modify firmware environment values	trusted users	trusted users	trusted users
Profile single process	trusted users	trusted users	trusted users
Profile system performance	trusted users	trusted users	trusted users
Replace a process level token	(no one)Do not assign to any user.	(no one)Do not assign to any user.	(no one)Do not assign to any user.
Restore files and directories	trusted users	trusted users	trusted users
Shut down the system	trusted users	(anyone)	(anyone)
Take ownership of files or other objects	trusted users	trusted users	trusted users
Recommended user rights settings			

Reference: Microsoft/technet/security/c2config
Reference: Mastering Windows NT Server 4 5th edition

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**