Global Information Assurance Certification Paper

Track 6 assignment – Option 1 - Developments in securing NT

1. To secure Windows NT against "Null Session" exploit

When a user uses an application to access data or services on remote Win NT computers, the user's username and password is sent to the remote machine to log in. If the user log in is unsuccessful, some applications try to log in using both the username and password as single null character. A session established in this manner is called "Null Session". NT users can not manually use null characters as username and passwords to access remote services or data. This functionality is built into various Win NT applications and services.
Though the functionality of "Null Sessions" is limited, it has opened security holes on Win NT systems.
A null session can be used

- To list all the users and groups in a NT domain from a remote machine using anonymous access
- To access shares
- To access the named pipes

Prevent Null Sessions from listing user accounts

To prevent the null sessions from listing users and groups from a domain, following registry change must be made on all of the domain controllers of the domain.
If the value does not exist, create one.

Hive: HKEY_LOCAL_MACHINE
Key: \System\CurrentControlSet\Control\LSA
Value: RestrictAnonymous
Value Type: REG_WORD
Value Data: 1

Use the following procedure to prevent Null Sessions from listing user accounts.

1. On a domain controller, run regedt32.exe (not regedit.exe) from 'start' menu or from 'command prompt'.
2. Navigate to the registry key : HKEY_LOCAL_MACHINE\ \System\CurrentControlSet\Control\LSA
3. Check if "RestrictAnonymous" value exists. If exists, double click on it. A "DWORD Editor" dialog pops up. Enter 1 in the **Data** field. Make sure that **Decimal** radio button is checked. Click OK.
4. If "RestrictAnonymous" does not exist, highlight key "LSA" and select "Edit\Add Value" menu.
5. Enter Value Name. Select Data Type as REG_WORD. Click OK.
6. A "DWORD Editor" dialog pops up. Enter 1 in the **Data** field. Make sure that **Decimal** radio button is checked. Click OK.
7. You should be able to see the "RestrictAnonymous" value listed under "LSA".

8. Repeat this procedure on all the Domain Controllers (Primary and Secondary) on your network.

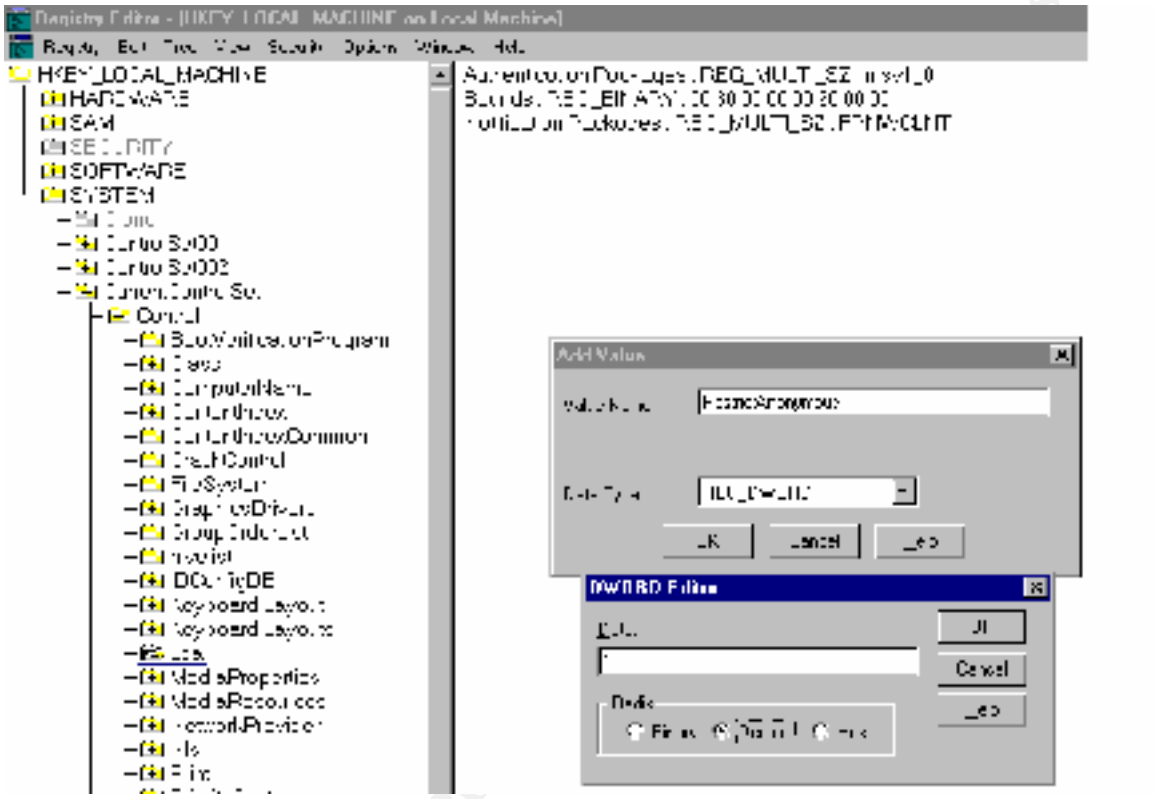


Figure 1: Add "RestrictAnonymous" value if it does not exist in the registry.

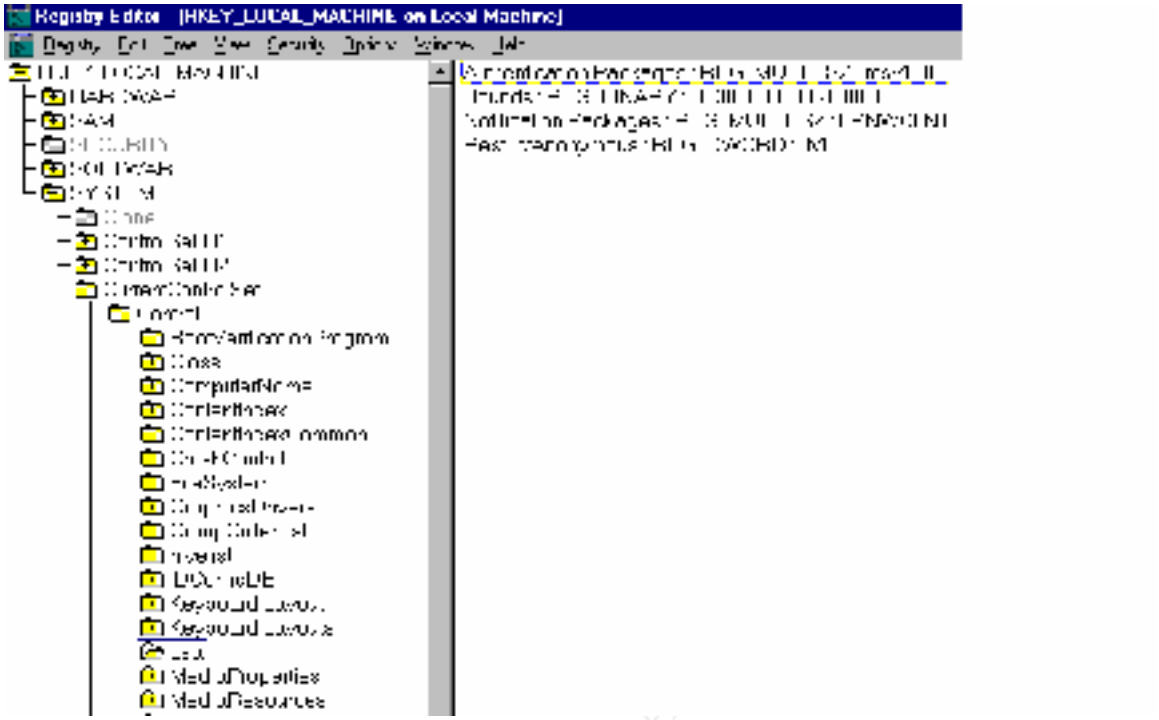


Figure 2: The newly created "RestrictAnonymous" value with data **1**.

Control Null Session access to shares

Null Session access to shared folders, can be controlled by setting appropriate values of "RestrictNullSessAccess" and "NullSessionShares" in the registry. If "RestrictNullSessAccess" value is set to 1, "Null Session" users can not any shares except those listed under "NullSessionShares" value in the registry.

Hive: HKEY_LOCAL_MACHINE
Key: \System\CurrentControlSet\Services\Lanmanserver\Parameters
Value: RestrictNullSessAccess
Value Type: REG_WORD
Value Data: 1

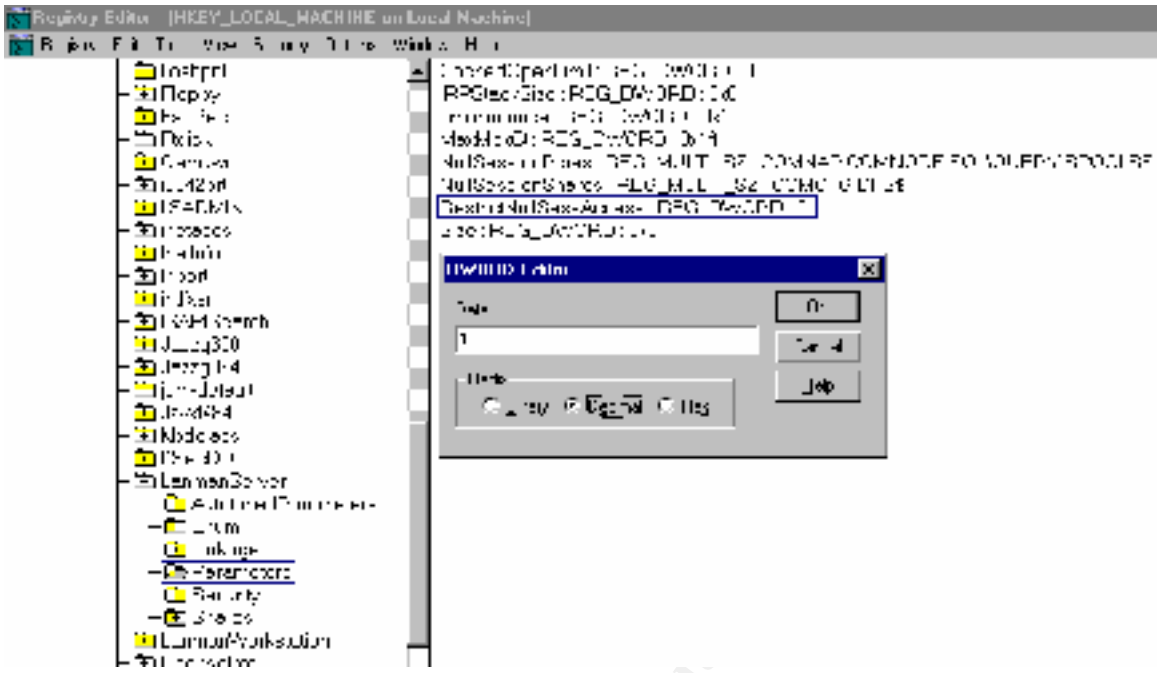


Figure 3: Modify "RestrictNullSession" access value to 1

When value of "RestrictNullSessAccess" is 1, "Null Session" users can not access shared folders even if they are shared to the "Everyone" group. The shares that need "Null Session" user access to override the above, must be listed under registry value "NullSessionShares".

Hive: HKEY_LOCAL_MACHINE
Key: \System\CurrentControlSet\Services\Lanmanserver\Parameters
Value: NullSessionShares
Value Type: REG_MULTI_SZ
Value Data: <one or more shares>

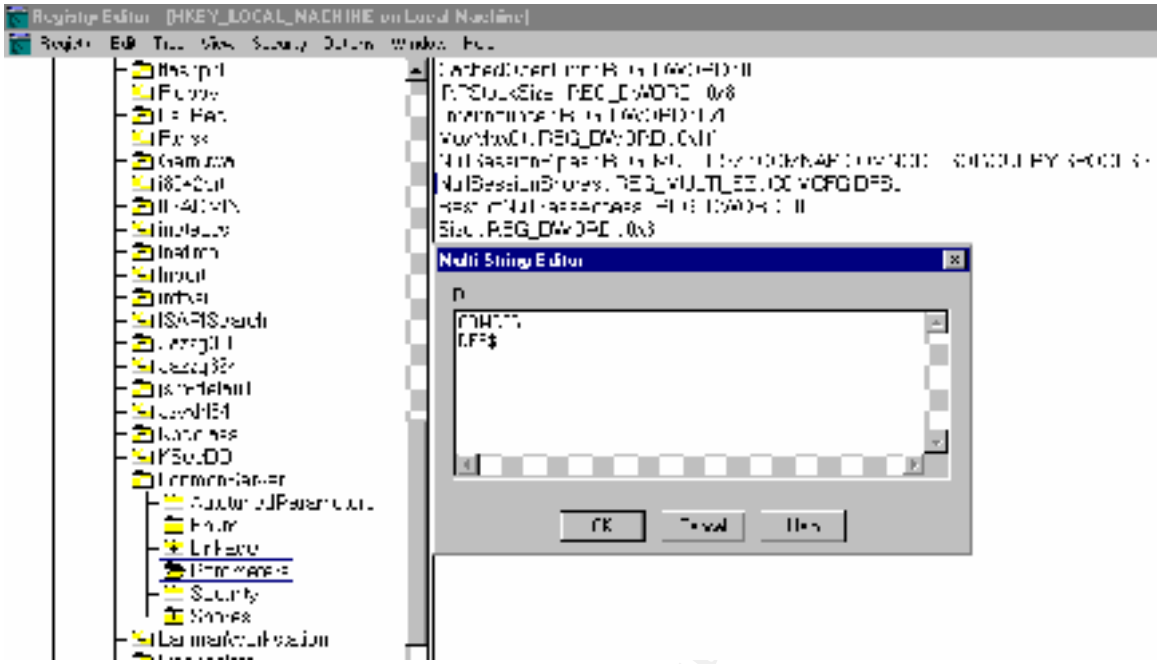


Figure 4: Add list of exception shares in "NullSessionShares" value.

The share names listed under registry value "NullSessionShares" are accessible to "Null Session" users when that share permits access to the "Everyone" group.

Control Null Session access to Named Pipes

A named pipe is an Inter-Process Communications (IPC) mechanism that is accessible as a share name to which Win NT remote services and applications can connect. Named pipe is implemented as a Named Pipe File System (NPFS). NPFS resides in the memory address space of the processes, which want to communicate with each other.
The UNC pathname format of named pipes is \\servername\Pipe\pipename where share name "pipe" is built into the Win NT OS.
Examples:

- \\servername\pipe\Netlogon
- \\servername\pipe\Winreg
- \\servername\pipe\SQL\QUERY

Null Session access to Named Pipes, can be controlled by setting appropriate values of "RestrictNullSessAccess" and "NullSessionPipes" in the registry.

Set "RestrictNullSessAccess" value to 1 as described in the last section.
"NullSessionPipes" registry value lists the named pipes, which should be accessible to the "Null Session" users. Any named pipe on this list is open to the anonymous users.

Hive: HKEY_LOCAL_MACHINE
Key: \System\CurrentControlSet\Services\Lanmanserver\Parameters

Value: NullSessionPipes
Value Type: REG_MULTI_SZ
Value Data: <one or more shares>

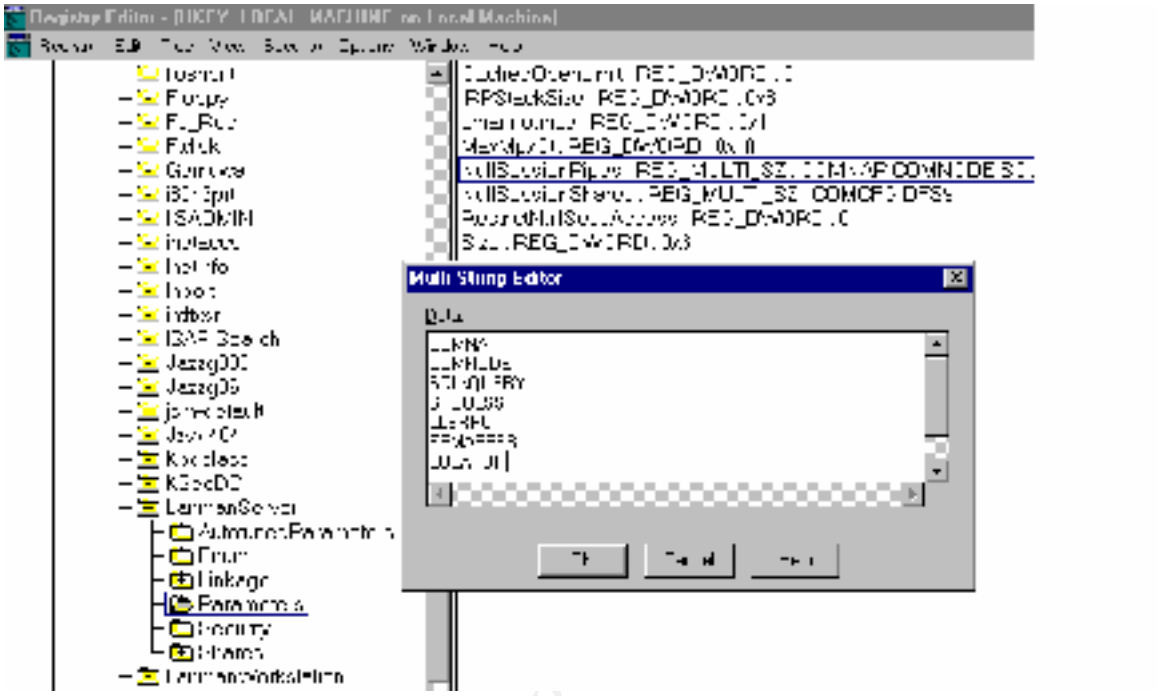


Figure 5: Add the named pipes accessible to "Null Session" users under the "NullSessionPipes" list value.

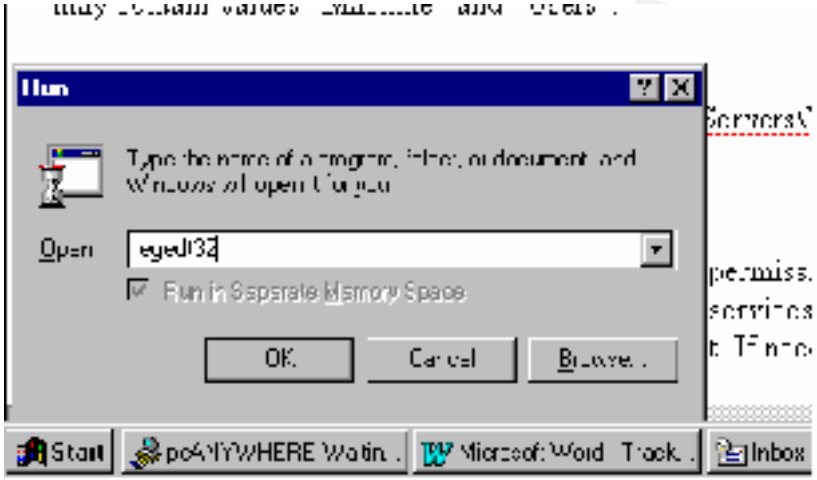
2. Restrict remote(Network) access to Win NT registry

By default, on Win NT Server, only administrators can access the registry. If a Win NT workstation or a Win NT server is compromised on a Win NT network, it is possible for a hacker to run utilities that dump the contents of registries of remote machines.
To control remote access permissions to a Win NT system registry, one can assign desired permissions on the "**Winreg**" key located at:

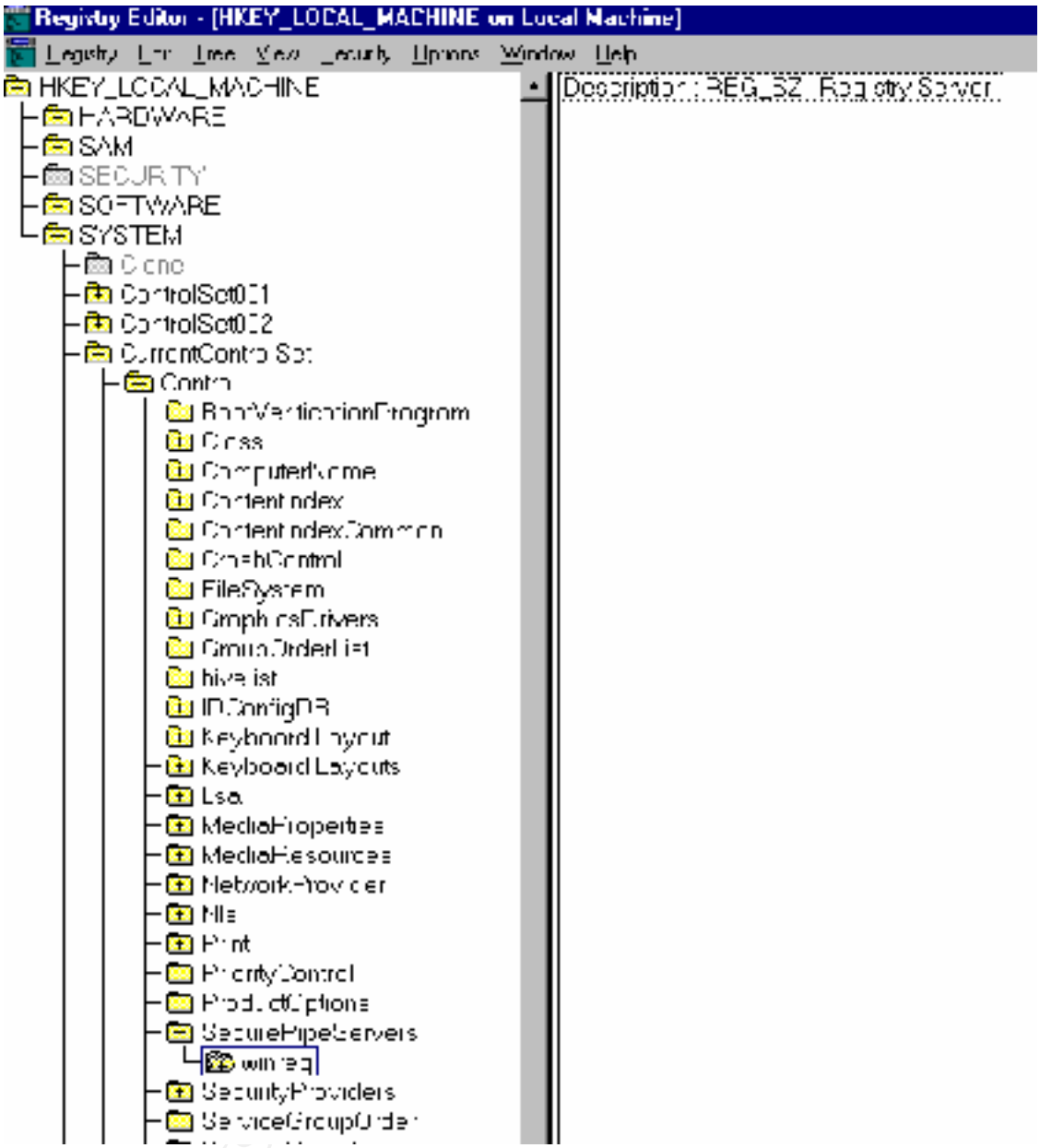
Hive: HKEY_LOCAL_MAHCINE
Key: \system\currentcontrolset\control\SecurePipeServers\Winreg

Win NT OS interprets the permissions set on the **Winreg** key as the permissions needed for controlling remote access.
Use the following steps to configure the registry remote access:

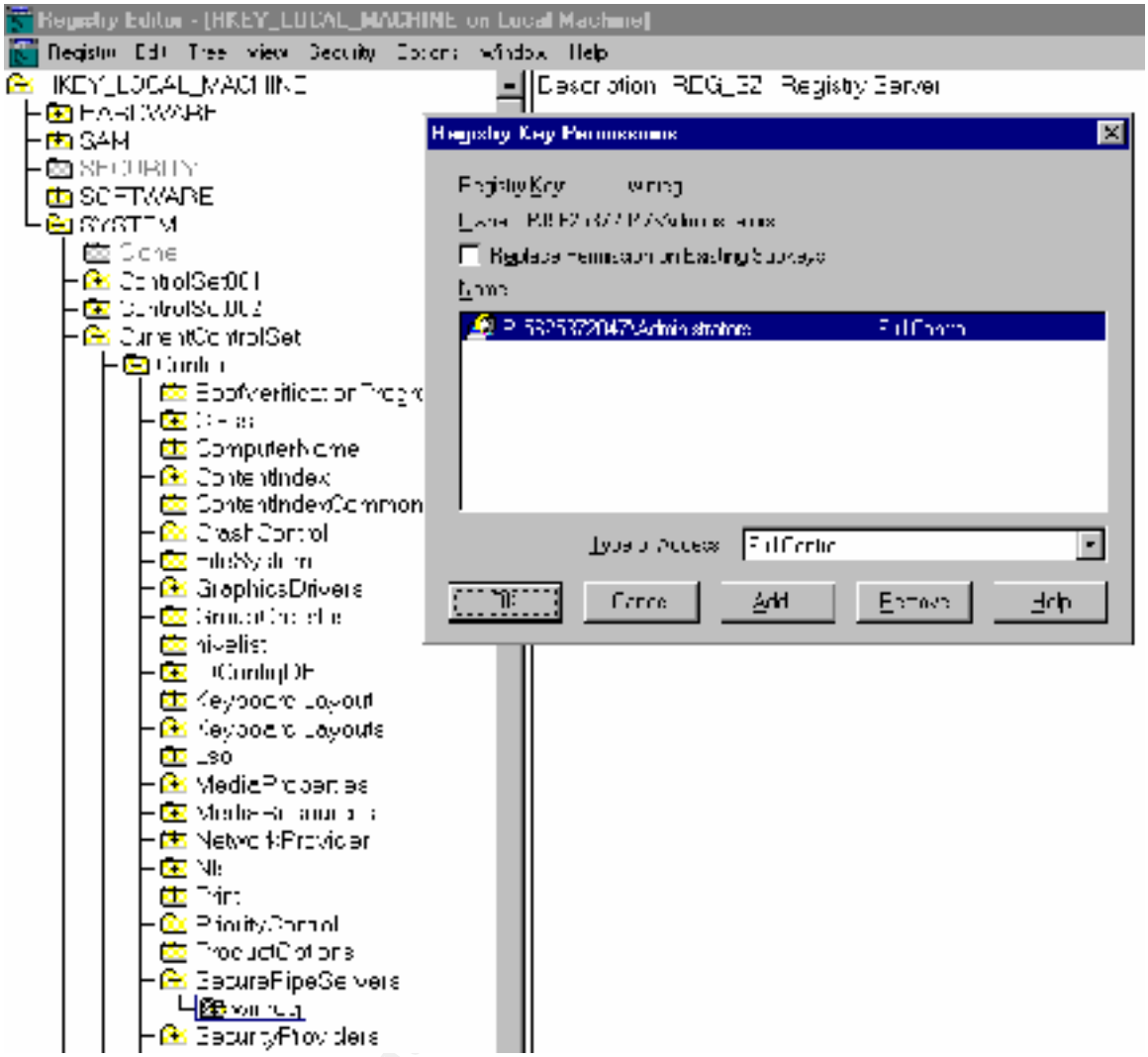
1. Start **regedt32.exe** from start menu or command prompt.



2. Navigate to the key HKEY_LOCAL_MAHCINE\
\system\currentcontrolset\control\SecurePipeServers\Winreg.



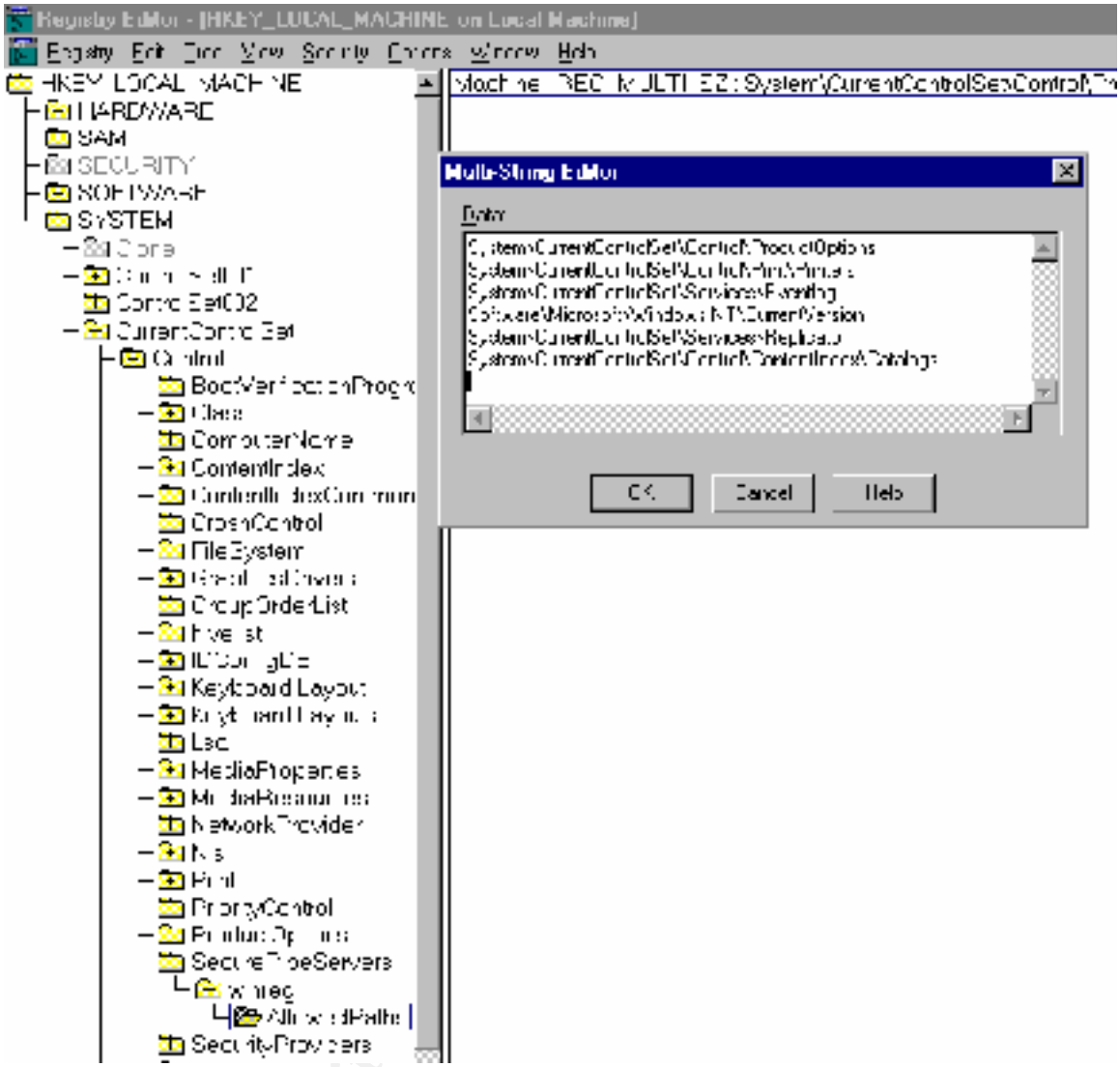
3. Highlight the "**Winreg**" key.
4. Pull down the **Security** menu. In **Security** menu, select **permissions**. A 'Registry Key Permissions' dialog is displayed as shown below.



5. The permissions set in this dialog are the permissions for remote users.

Some of the Win NT registry paths might have to be excluded from the above restriction for proper functioning of some system services. This can be achieved by setting using values listed under “AllowedPaths” subkey under “Winreg” key. “AllowedPaths” subkey may contain values “Machine” and “Users”.

Hive: HKEY_LOCAL_MAHCINE
Key: \system\currentcontrolset\control\SecurePipeServers\Winreg
Value Names: Machine or Users
Value Type: REG_MULTI_SZ



The “Machine” value lists all the exceptions to the permissions assigned to the “Winreg” key. The exceptions can be used by remote system services for both read and write access. “Machine” value has a default exception list. If needed, paths can added to this list.

The “Users” value is not available by default, it must be created manually. The “Users” value lists the registry paths that are accessible to the authenticated users even after setting permissions on the “Winreg” key.

3. Control access to the Schedule Service

The Schedule service executes programs and batch files automatically at scheduled times. The programs run by Schedule service operate under the security context of System Account. The programs and batch files run by Scheduler service have unlimited access to the Win NT OS. The Schedule Service can be started and stopped from Services Applet in the Control Panel. AT.exe or a Resource Kit GUI utility WINAT.exe is used to submit jobs to the Schedule service.
There are two threats created from miss-use of the Schedule service.

1. If a Win NT server is compromised, the attacker can Schedule any harmful commands at any time.
2. An attacker can read which jobs have been scheduled. Attacker can replace the programs or batch files scheduled to be executed, with his/her own malicious programs.

These threats can be reduced by

- Controlling job submission
- Controlling job listing
- Using fully qualified paths

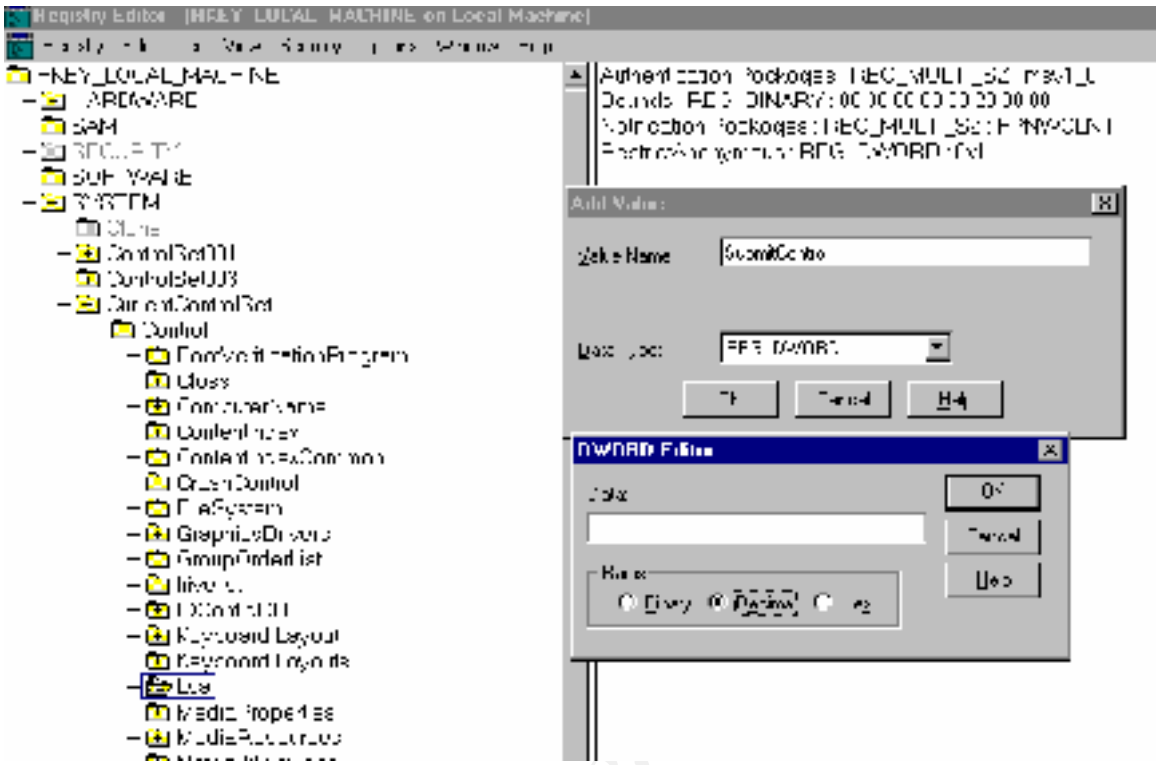
Controlling job submission

Only Administrators and Power Users groups can submit new jobs to the Schedule service. Add a new registry value "SubmitControl" to allow the Server Operators Group to be able to submit new jobs. Other groups and individual accounts are not permitted to submit jobs this way.

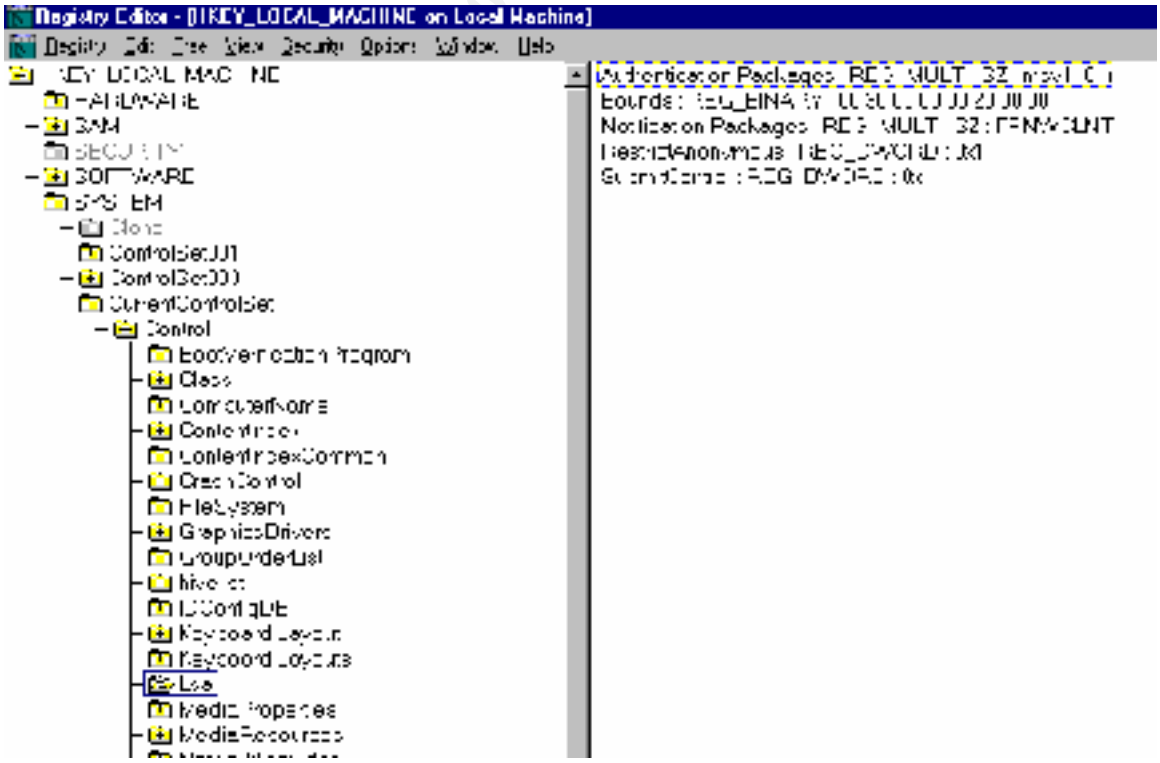
Hive: HKEY_LOCAL_MACHINE
Key: \System\CurrentControlSet\Control\LSA
Value: SubmitControl
Value Type: REG_WORD
Value Data: 1

Use the following procedure to add "SubmitControl" value in the registry

1. On a domain controller, run regedt32.exe (not regedit.exe) from 'start' menu or from 'command prompt'.
2. Navigate to the registry key : HKEY_LOCAL_MACHINE\ \System\CurrentControlSet\Control\LSA
3. Check if "SubmitControl" value exists. If exists, double click on it. A "DWORD Editor" dialog pops up. Enter 1 in the **Data** field. Make sure that **Decimal** radio button is checked. Click OK.
4. If "SubmitControl" does not exist, highlight key "LSA" and select "Edit\Add Value" menu.
5. Enter Value Name. Select Data Type as REG_WORD. Click OK.



6. A "DWORD Editor" dialog pops up. Enter 1 in the **Data** field. Make sure that **Decimal** radio button is checked. Click OK.
7. You should be able to see the "SubmitControl" value listed under "LSA".



Control job listing

Assign appropriate permissions on registry key HKEY_LOCAL_MACHINE\
\System\CurrentControlSet\Services\Scheule to control who can list the scheduled jobs. Only Administrators and System account should have access to this key.

Use the following procedure to control the permissions to Scheduled job listing:

1. On a domain controller, run regedt32.exe (not regedit.exe) from 'start' menu or from 'command prompt'.
2. Navigate to the registry key : HKEY_LOCAL_MACHINE\
\System\CurrentControlSet\Services\Schedule
3. Highlight the Schedule key.
4. Select Security menu. Select Permissions sub-menu. The 'Registry Key Permissions' dialog is displayed. It lists the current permissions set on the 'Schedule' key.

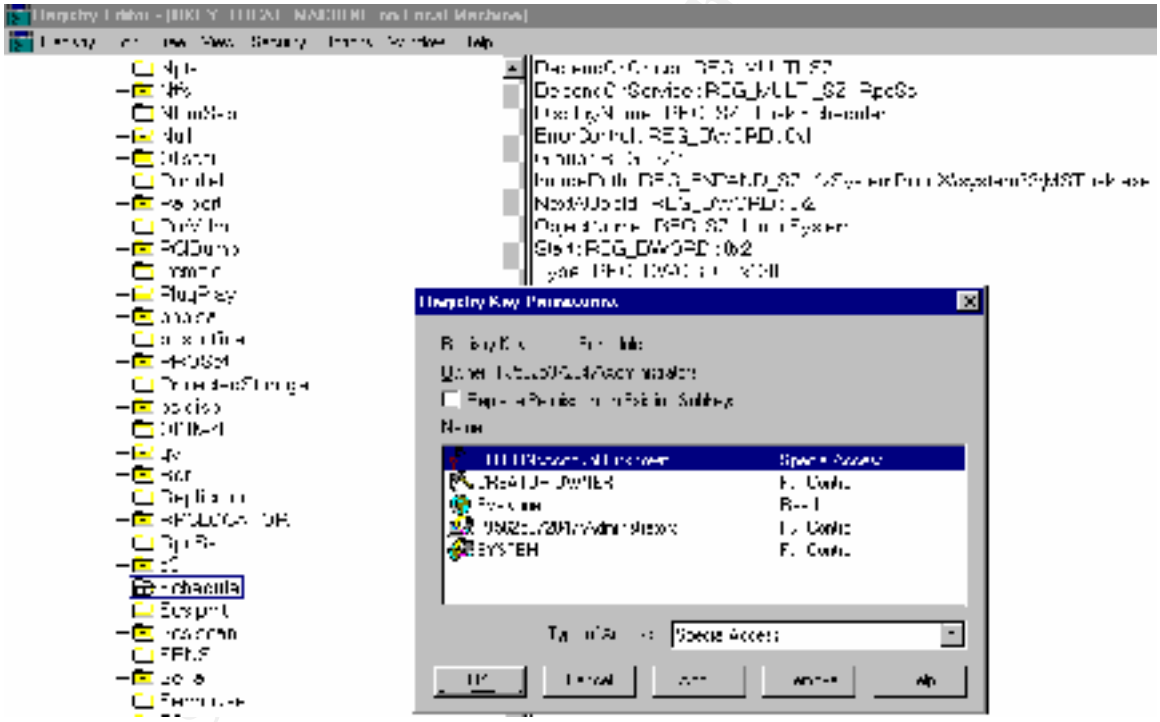


Figure 6: The default permissions on the 'Schedule' key

5. Modify the default permissions on the 'Schedule' key to permit only the Administrator and System account to list the schedule jobs.

Use Fully Qualified Paths

If executable programs or batch files are scheduled without specifying the full path, the Schedule service searches the folders specified in the PATH environment variable. An attacker can place malicious programs with the same names in the folders, which fall appear in the PATH list. The Schedule service will find the malicious program first and execute it instead of the correct program.

Last Updated: July 24th, 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**