



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>

Option 1 – Developments in securing NT

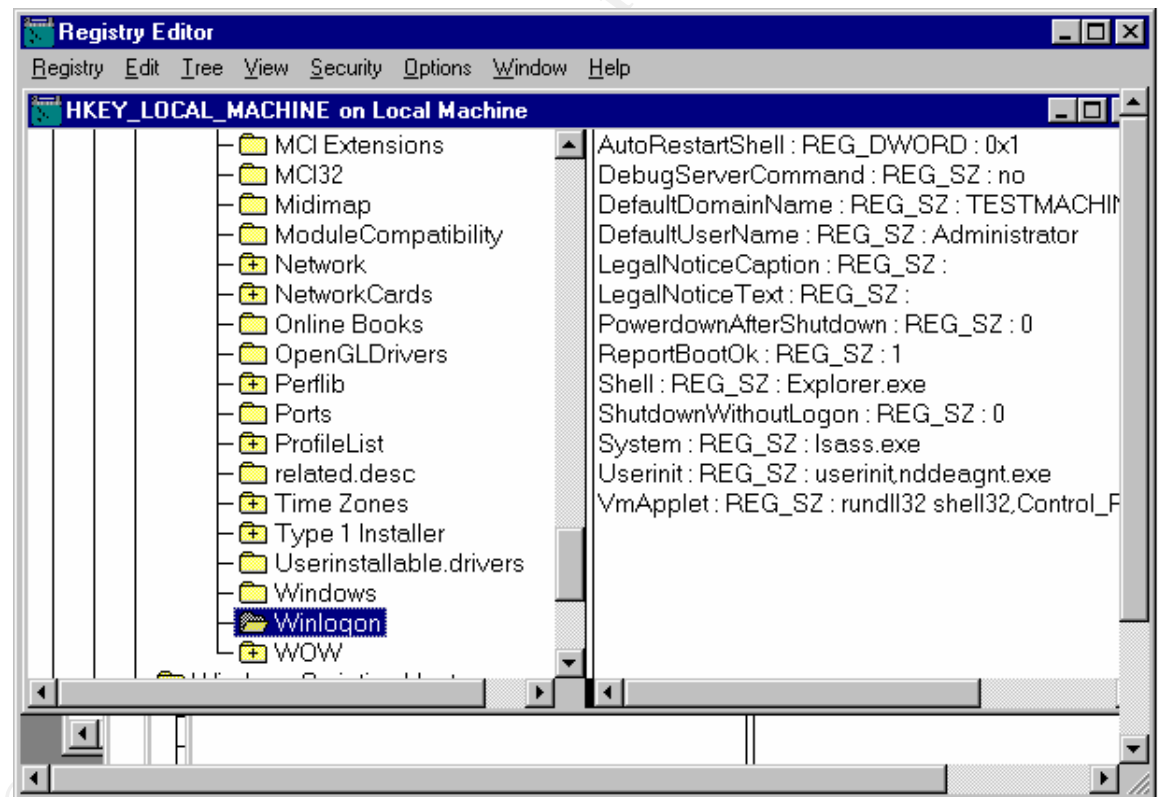
Author – Raymond Chan

SANS San Jose 2000 – Windows NT Security GIAC Training

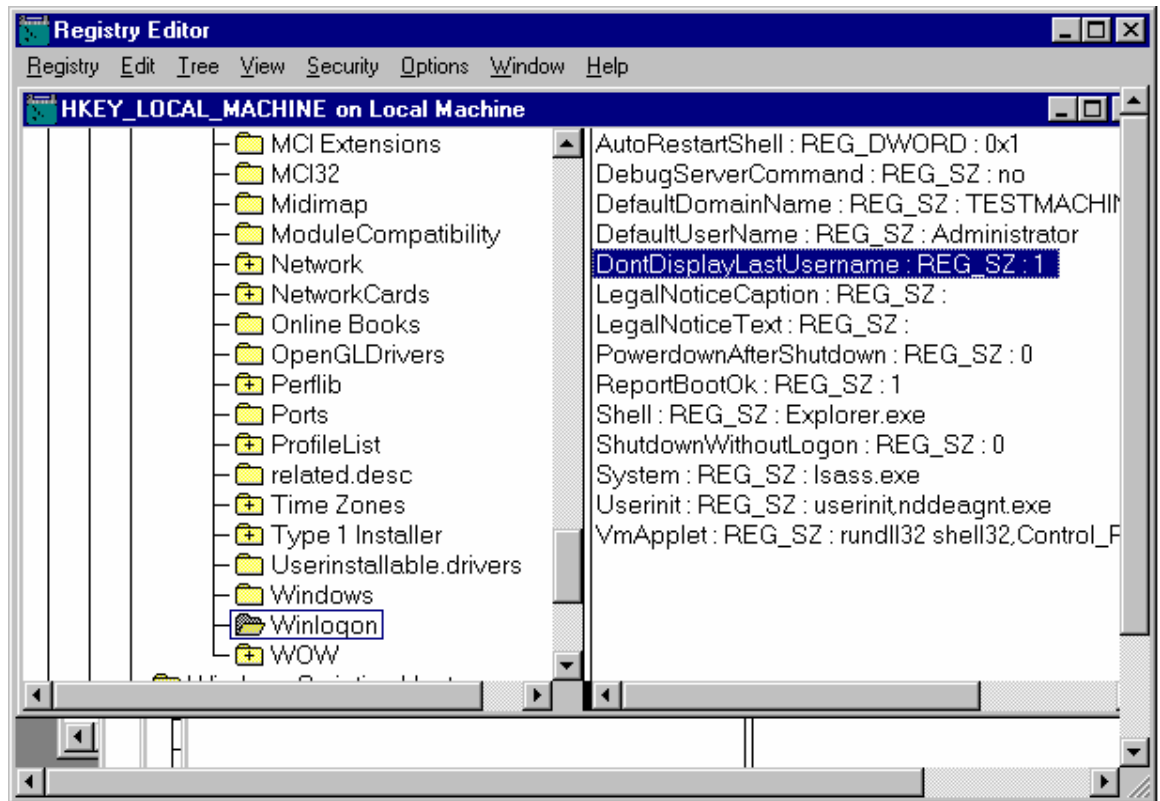
A Step-By-Step Guide for Setting Registry Keys

A. Disable the display of the last logged on username

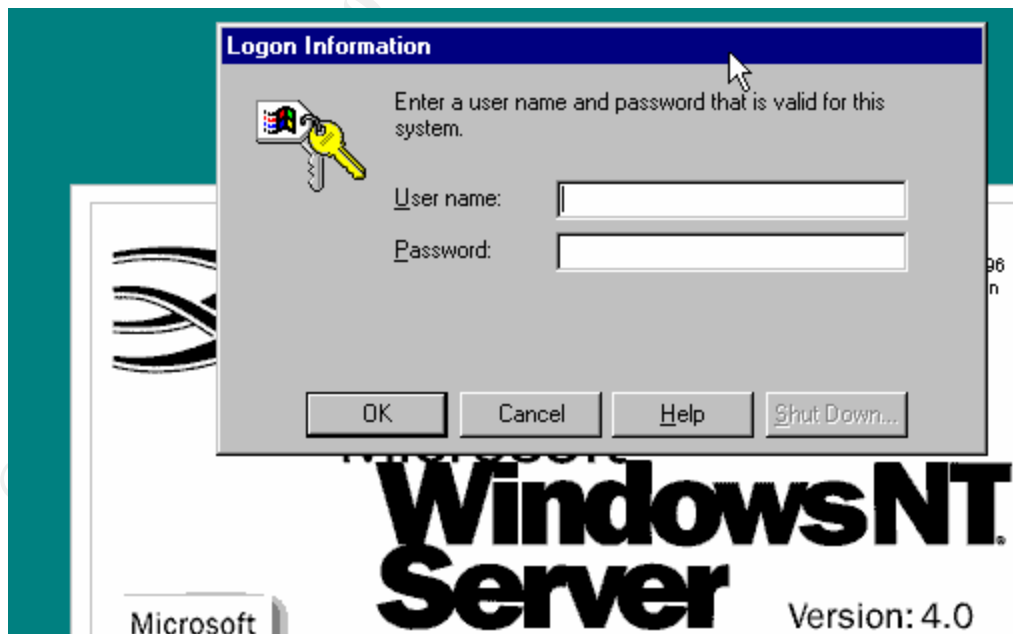
1. Run regedt32 using Start->Run
2. Select the hive HKEY_LOCAL_MACHINE
3. Select Software\Microsoft\Windows NT\CurrentVersion\Winlogon. The screen shall look like:



4. Select Edit->Add Value
5. Enter DontDisplayLastUsername for the value name and REG_SZ for the data type. Press OK.
6. Enter '1' in the string edit box and press OK
7. The screen shall look like:

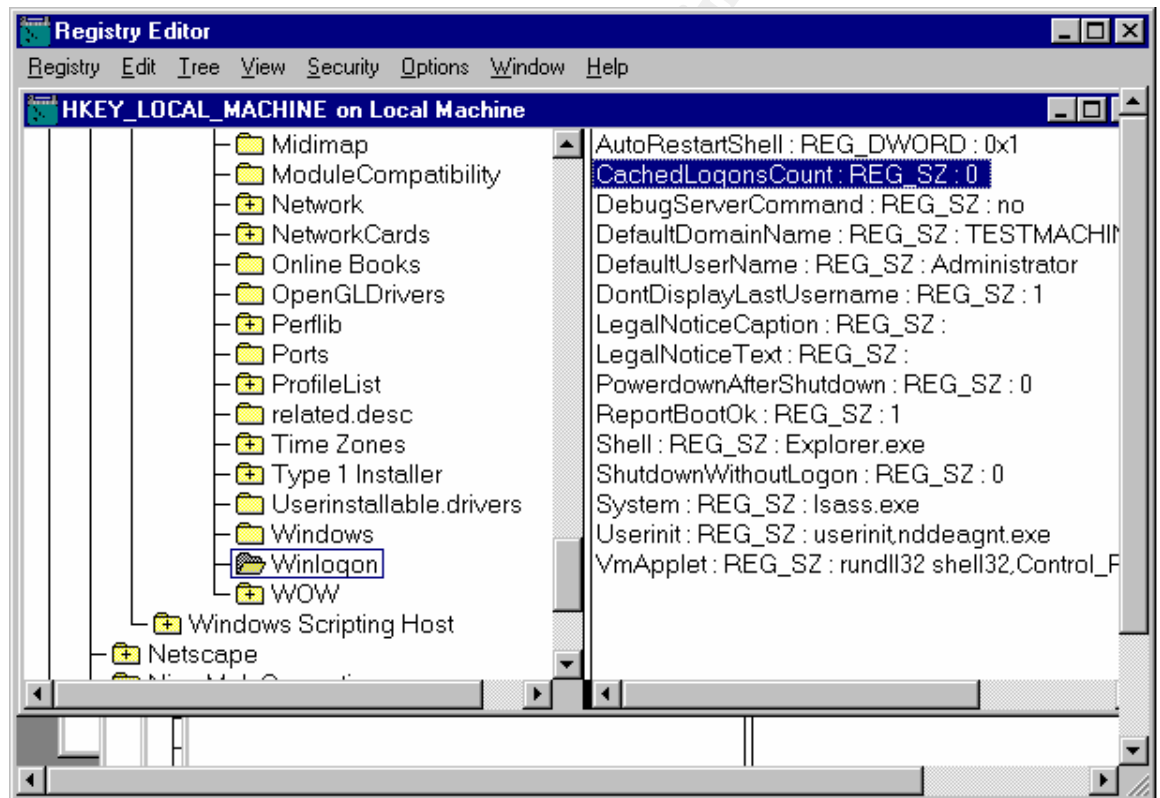


8. Now the logon box will not show the last logged on username.



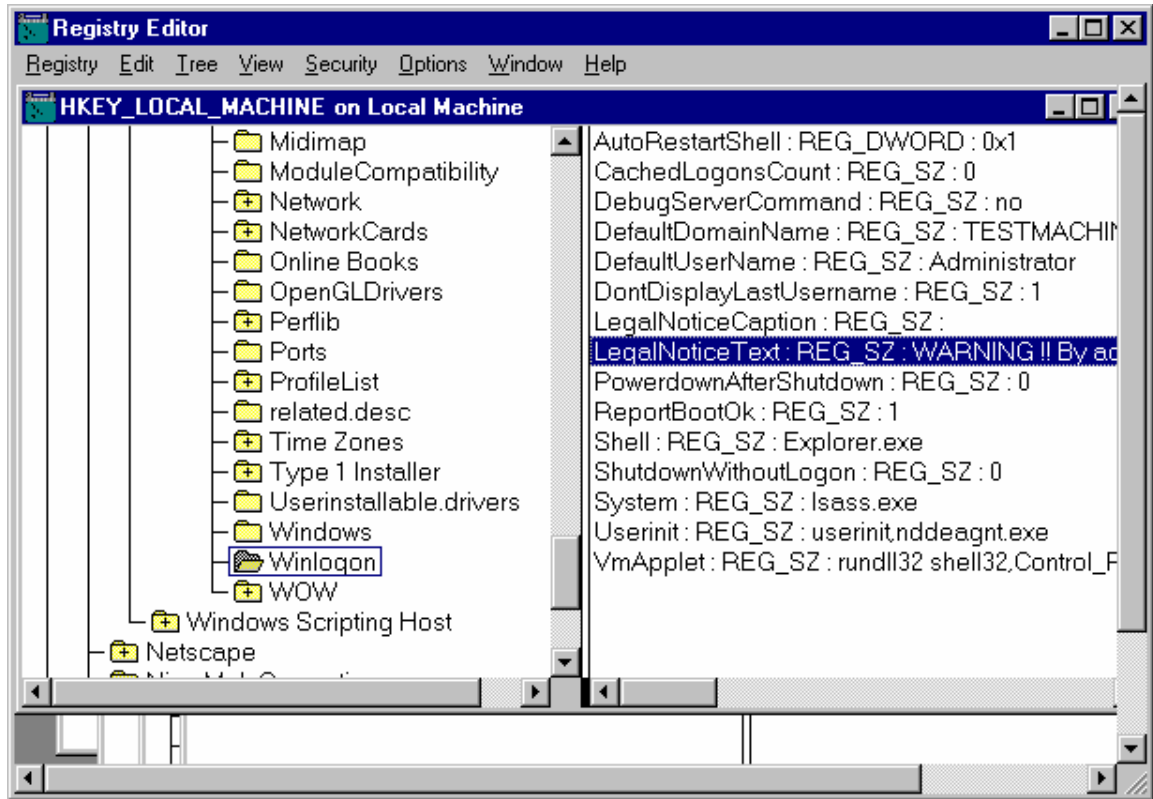
B. Disable caching of logon information

1. Run regedt32 using Start->Run
2. Select the hive HKEY_LOCAL_MACHINE
3. Select Software\Microsoft\Windows NT\CurrentVersion\Winlogon.
4. Select Edit->Add Value
5. Enter CachedLogonsCount for the value name and REG_SZ for the data type. Press OK.
6. Enter '0' in the string edit box and press OK.
7. The screen shall look like:



C. Use the logon message to warn intruders

1. Run regedt32 using Start->Run
2. Select the hive HKEY_LOCAL_MACHINE
3. Select Software\Microsoft\Windows NT\CurrentVersion\Winlogon.
4. Select Edit->Add Value
5. Enter LegalNoticeText for the value name and REG_SZ for the data type. Press OK.
6. Enter a logon message that you want to warn intruders and press OK.
7. The screen shall look like:

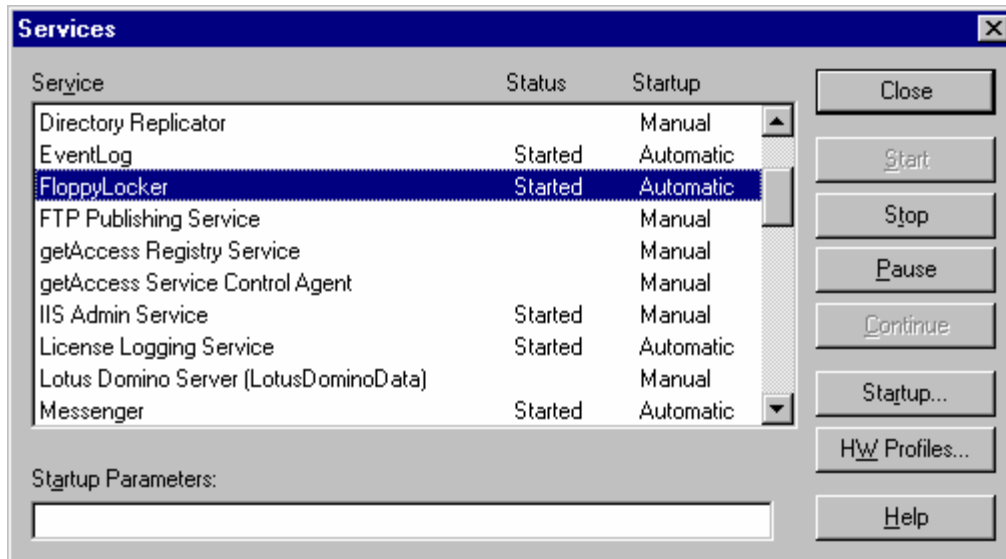


8. Now a logon message will be displayed before each logon.



D. Disable floppy disk drives for non-administrators

1. Install NT Resource Kit.
2. Run cmd using Start->Run
3. Enter "instsrv FloppyLocker c:\ntreskit\floplock.exe" assuming the resource kit is installed at the default location.
4. Start the FloppyLocker service using Start->Settings->Control Panel->Services as shown below or reboot since the FloppyLocker will be started on bootup.



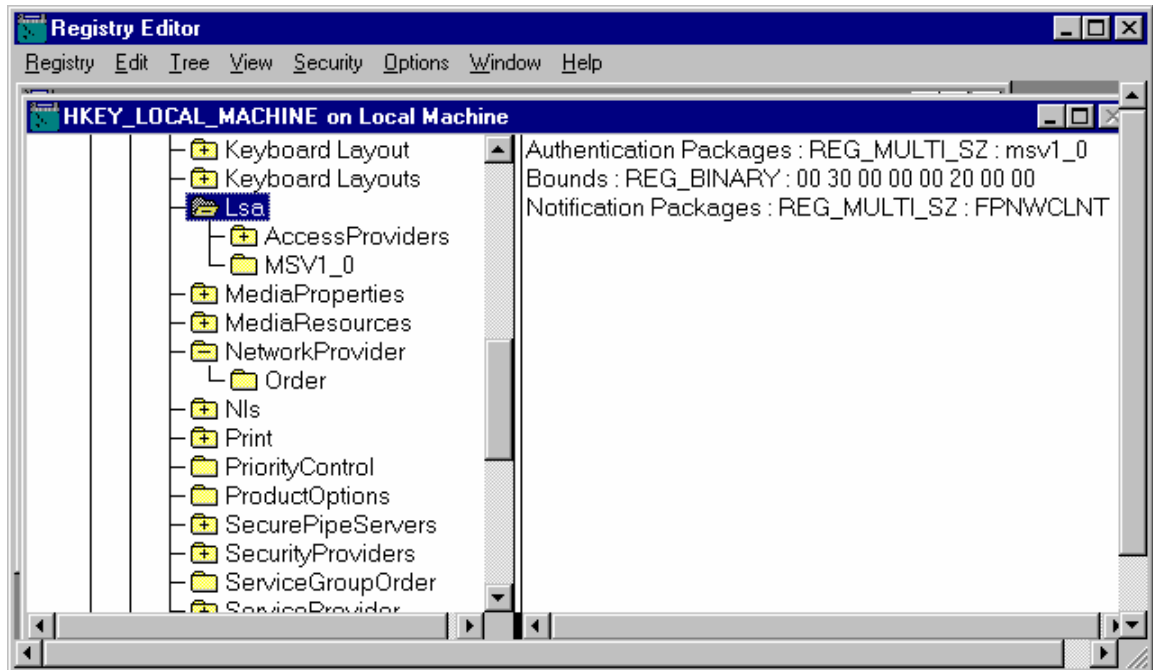
5. Now logoff and re-login as an ordinary user instead of administrator.
6. Any attempts to access the floppy drive will result in errors:



E. Avoid the Netware DLL Trojan horse

1. Run regedt32 using Start->Run
2. Select the hive HKEY_LOCAL_MACHINE
3. Select SYSTEM\CurrentControlSet\Control\Lsa
4. The screen shall look like:

© SANS Institute 2000 - 2002

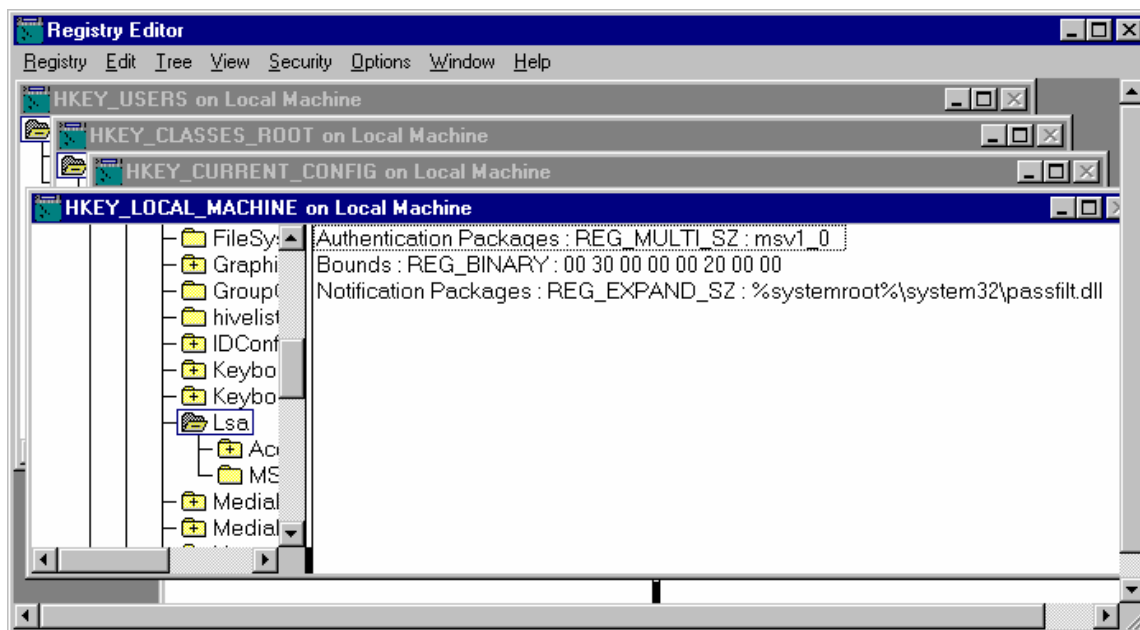


5. Select "Notification Packages"
6. Delete the "Notification Packages" value using Edit->Delete

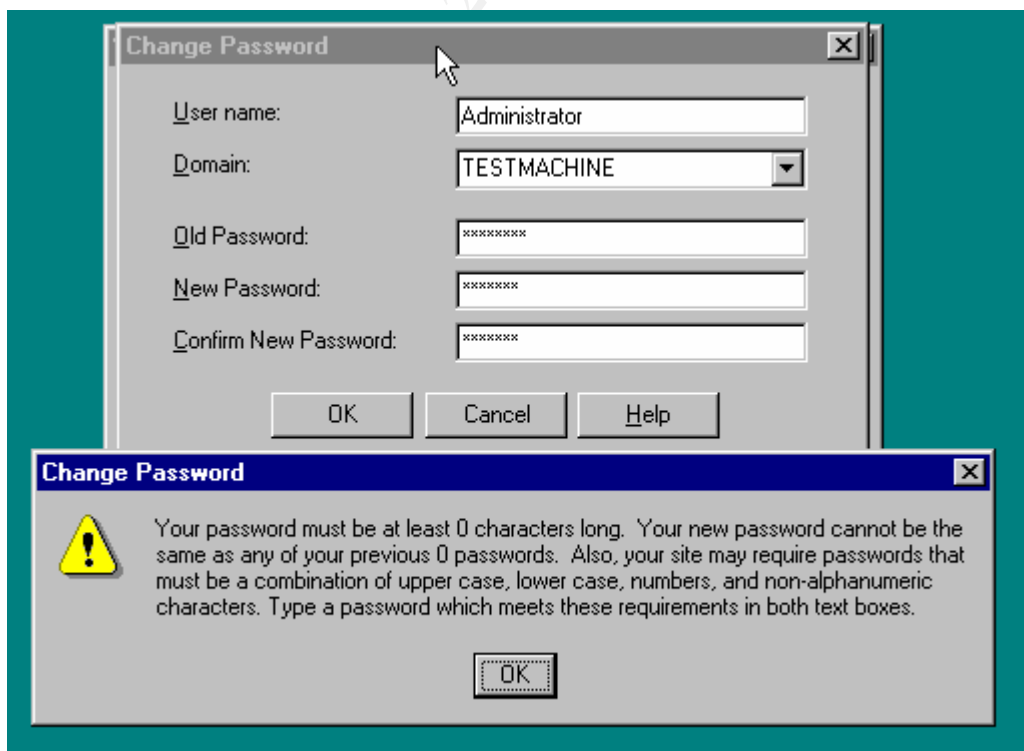
F. Enforce strong passwords

1. Run regedt32 using Start->Run
2. Select the hive HKEY_LOCAL_MACHINE
3. Select SYSTEM\CurrentControlSet\Control\Lsa
4. Select Edit->Add Value
5. Enter "Notification Packages" for the value name and REG_EXPAND_SZ for the data type. Press OK.
6. Enter %systemroot%\system32\passfilt.dll in the string edit box and press OK.
7. The screen shall look like:

© SANS Institute 2000 - 2002, All rights reserved.

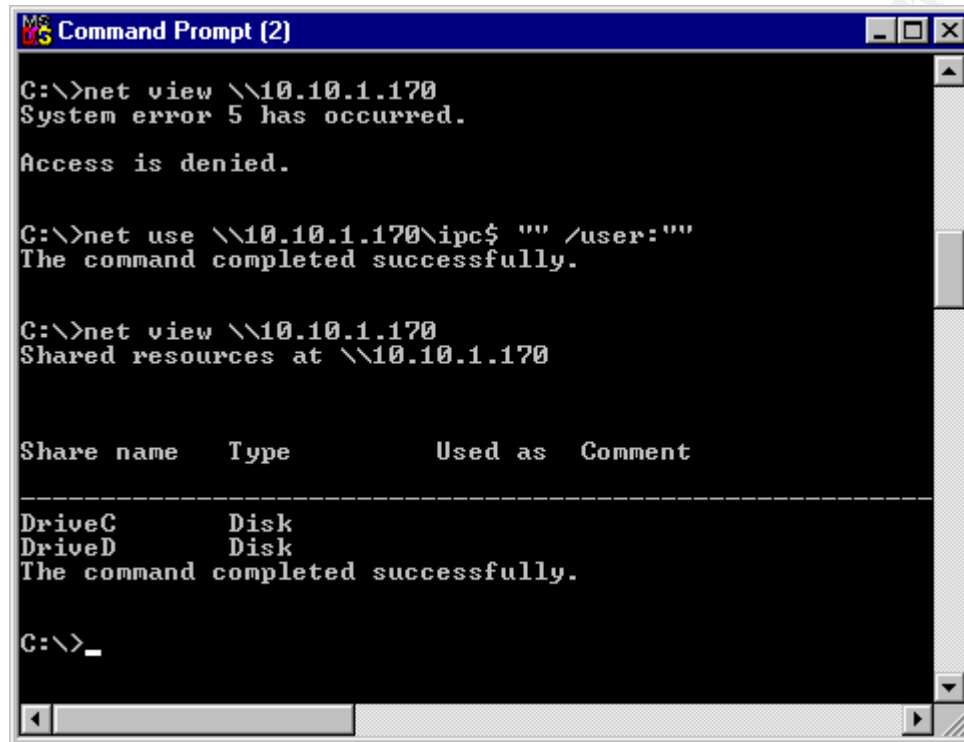


8. Exit regedt32 and reboot the system.
9. After the system comes up, log in and try to change password using Control-Alt-Delete "Change Password" option. If the new password does not satisfy the new password requirement, an error message will be generated as follows:



G. Restrict anonymous logon

1. Verify “null session” has not been disabled in the system by performing the following command sequence in a command box on a remote NT machine. The NT server used for this example is at 10.10.1.170.



```
MS-DOS Command Prompt (2)
C:\>net view \\10.10.1.170
System error 5 has occurred.

Access is denied.

C:\>net use \\10.10.1.170\ipc$ "" /user:""
The command completed successfully.

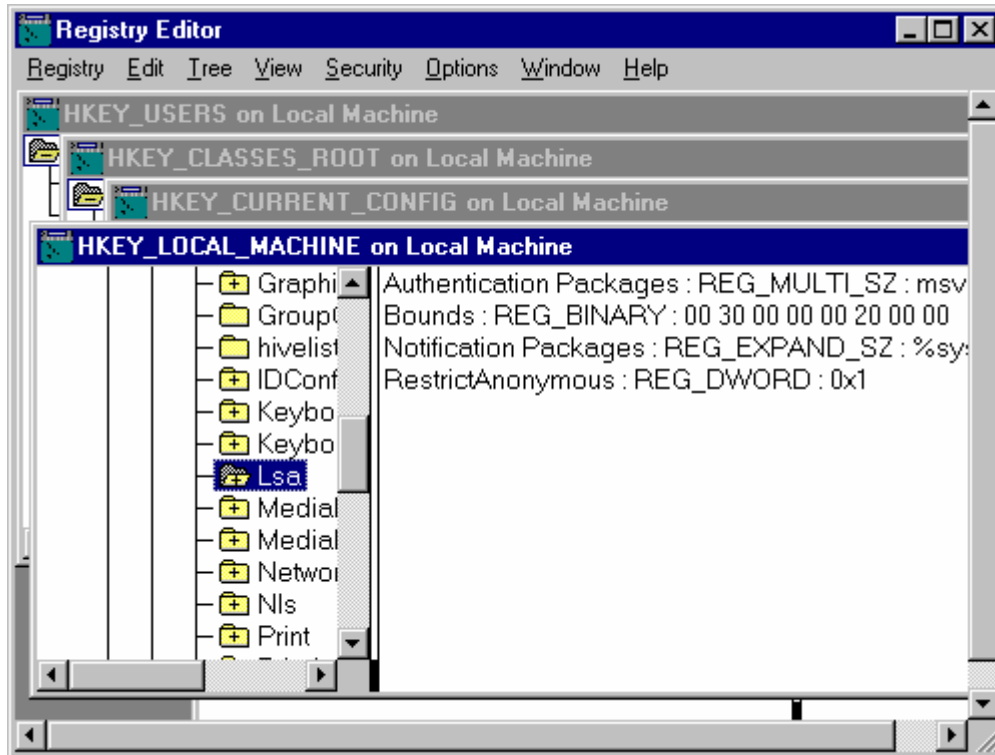
C:\>net view \\10.10.1.170
Shared resources at \\10.10.1.170

Share name      Type           Used as      Comment
-----
DriveC          Disk
DriveD          Disk
The command completed successfully.

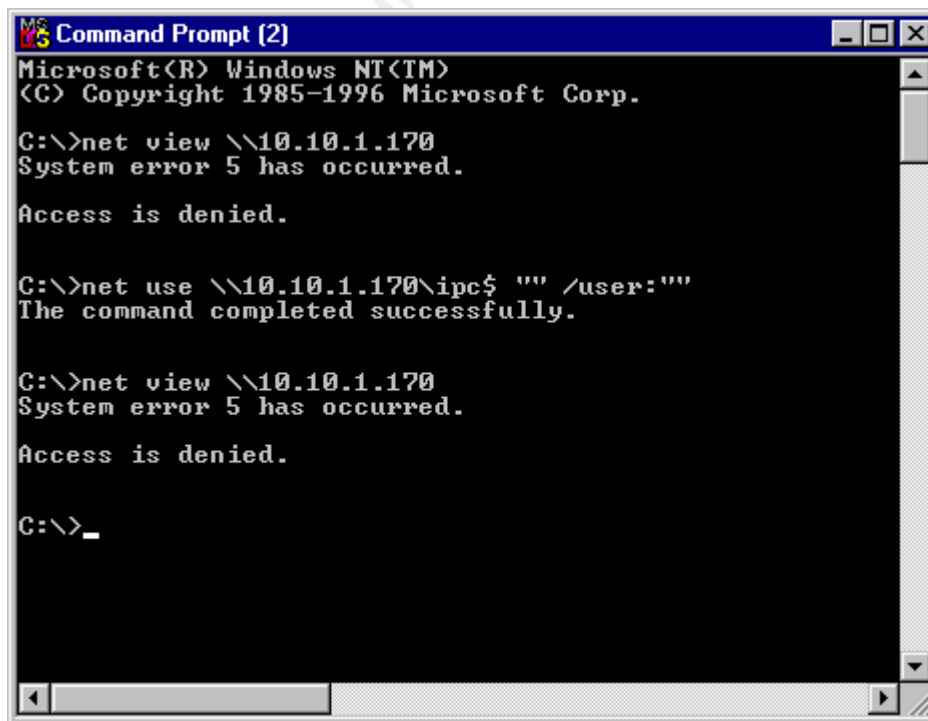
C:\>_
```

2. Run regedt32 using Start->Run
3. Select the hive HKEY_LOCAL_MACHINE
4. Select SYSTEM\CurrentControlSet\Control\Lsa
5. Select Edit->Add Value
6. Enter “RestrictAnonymous” for the value name and REG_DWORD for the data type. Press OK.
7. Enter “1” in the data edit box and press OK.
8. The screen shall look like:

© SANS Institute

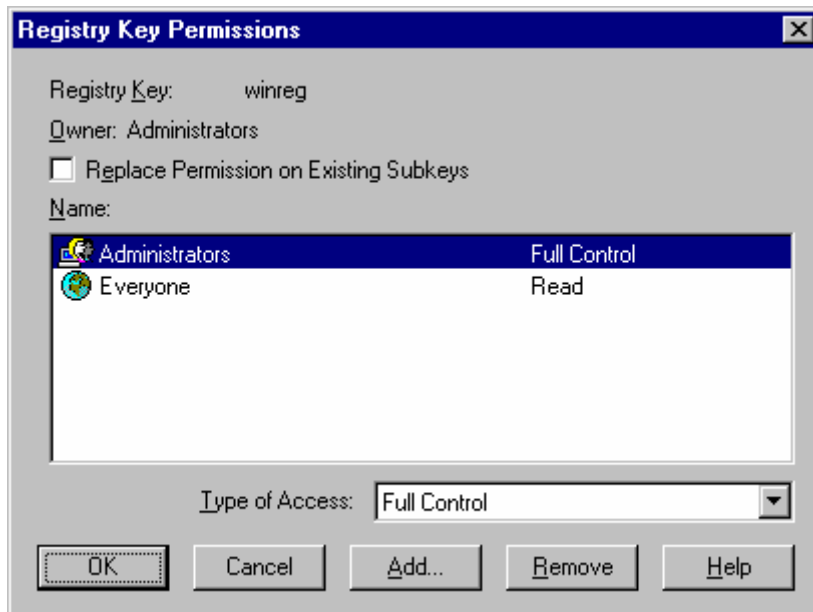


9. Now reboot the local NT server and remote machine.
10. Logon to the remote machine and try to setup a "null session" again.
11. This time an error message will be generated as follows:



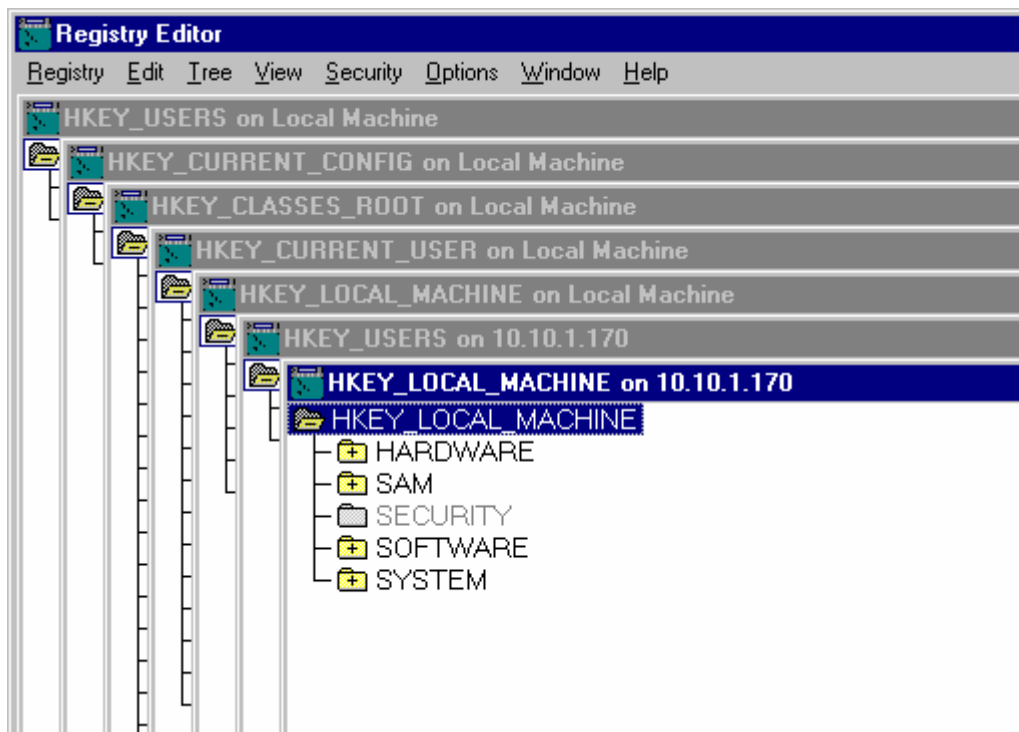
H. Control remote access to the registry

1. Run regedt32 using Start->Run
2. Select the hive HKEY_LOCAL_MACHINE
3. Select SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg
4. Select Security->Permissions
5. The screen shall look like:

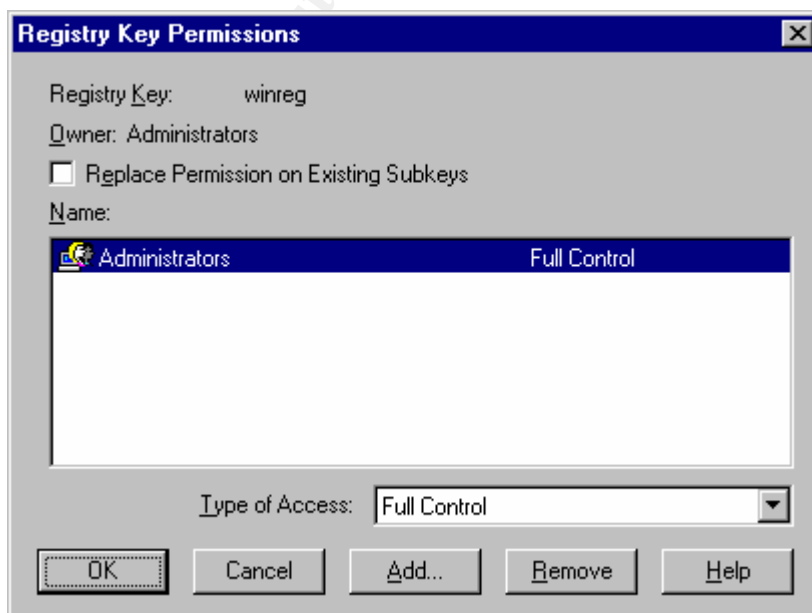


6. Log on to a remote computer and run regedt32.
7. Select Registry->Select Computer
8. Enter the IP address (10.10.1.170 in this example) or computer name of the NT server.
9. The screen shall look like:

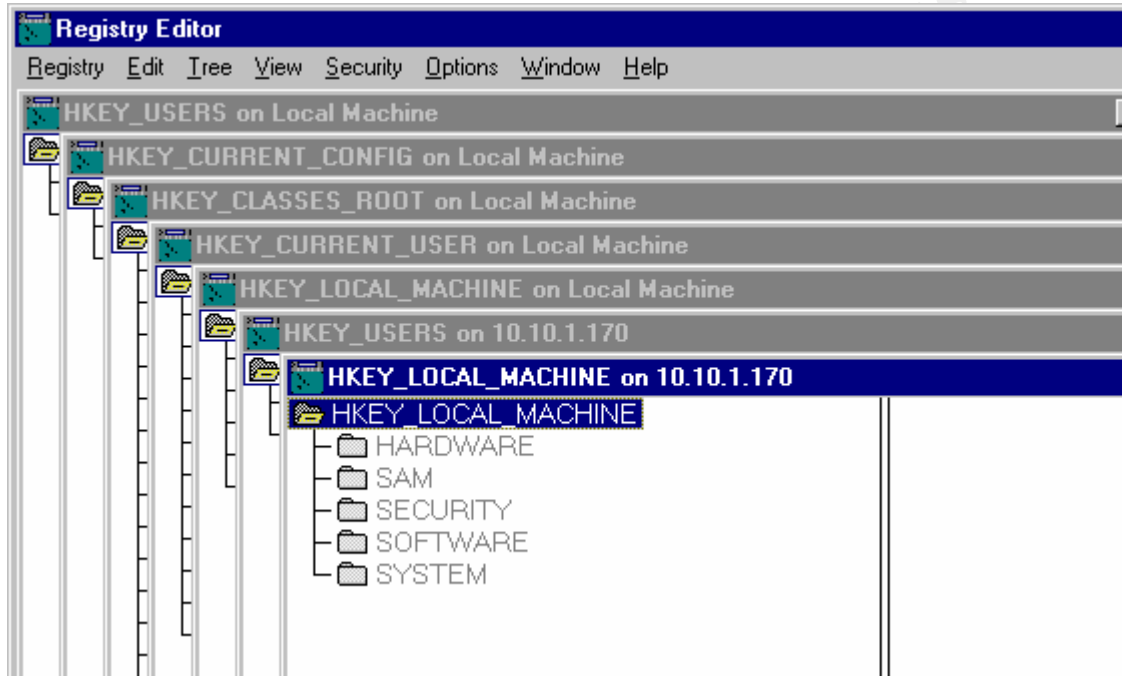
© SANS Institute 2000



10. The remote computer can display/update the registry on the NT server.
11. On the local NT server, run regedt32.
12. Select the hive HKEY_LOCAL_MACHINE
13. Select SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg
14. Select Security->Permissions
15. Remove all users except Administrators.
16. The screen shall look like:



17. Reboot the local and remote machines.
18. Access the NT server registry from the remote machine again using a non-administrator account.
19. The screen shall now look like:



20. The keys in the registry under HKEY_LOCAL_MACHINE for the NT server are now gray out indicating they are now not accessible remotely.

© SANS Institute 2000 - 2002

Upcoming Training

Click Here to
{Get CERTIFIED!}



| | | | |
|--|---------------------|-----------------------------|------------|
| SANS Cyber Defence Canberra 2017 | Canberra, Australia | Jun 26, 2017 - Jul 08, 2017 | Live Event |
| 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 06, 2017 | vLive |
| Secure DevOps Summit & Training | Denver, CO | Oct 10, 2017 - Oct 17, 2017 | Live Event |
| San Francisco Winter 2017 - SEC505: Securing Windows and PowerShell Automation | San Francisco, CA | Nov 27, 2017 - Dec 02, 2017 | vLive |
| SANS San Francisco Winter 2017 | San Francisco, CA | Nov 27, 2017 - Dec 02, 2017 | Live Event |
| SANS Cyber Defense Initiative 2017 | Washington, DC | Dec 12, 2017 - Dec 19, 2017 | Live Event |
| SANS OnDemand | Online | Anytime | Self Paced |
| SANS SelfStudy | Books & MP3s Only | Anytime | Self Paced |