

Module 9 Lab Host System Hardening

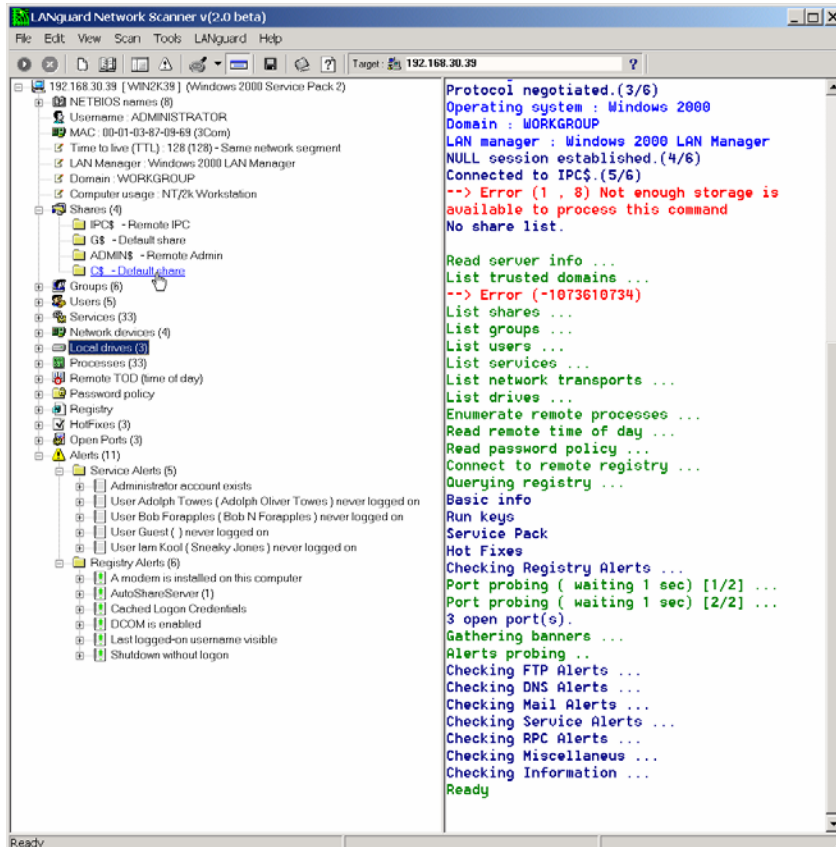
Background: This Lab reinforces the concepts of host system hardening. Students will discover vulnerabilities of systems and then apply techniques to harden and secure them.

Requirements/assumptions:

- Windows NT 4.0/2000
- Freeware version of Languard network scanner 2.0 (www.languard.com)
- Students must be logged in as Administrator
- Internet access
- Students must be split into pairs (partners) for portions of this lab

Exercise 1 – Enumerate system vulnerabilities

1. Open Languard Network Scanner
2. In the Target area, enter the IP address of your partner's computer—you can discover this by clicking Start/Run; then type cmd, then type ipconfig at the command prompt
3. In Languard, click the play button (▶) to start the scan
4. When the scan has finished, inspect the output in the left column. Notice that the following items, among others, have been scanned and are reported: users, services, processes, and alerts.



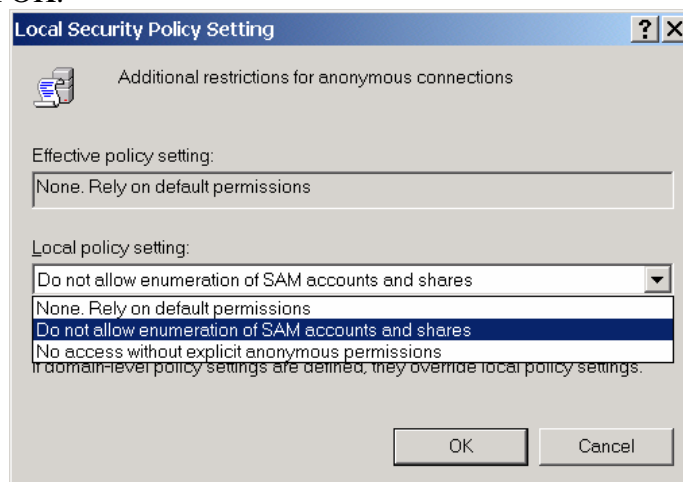
Module 9 Lab Host System Hardening

5. Click the + sign next to Shares. You may see the default share listed there (C\$). If this is the case, double-click it to open that share. When Languard finds the default share on a system, it can potentially be explored depending on that system's registry settings.
6. Briefly review the other scan result items. This gives you an idea of the current state of (or lack thereof) hardening on your host.
7. Select File\Save results (HTML) and then click Save --this is so you can compare the pre-hardening results with the scan you'll perform after you've hardened the system.

Exercise 2 – Restrict Anonymous connections

In the previous exercise, Languard network scanner took advantage of a vulnerable default registry setting in Windows NT 4.0/2000 that allows anonymous (null) connections to be established. As you saw in that exercise, anyone can gain access to another (remote) host's C: drive and do anything they want with it—default permissions for C: are Everyone/Full Control. In the following exercise, you'll make edits to the Windows registry that will harden/secure the system from this vulnerability.

- A. If you are using a Windows 2000 machine (NT 4.0 skip to B), follow the below steps:
1. Click Start/Settings/Control Panel/Administrative Tools/Local Security Policy. Under Local Policies, Security Options, double click *Additional restrictions for anonymous connections*.
 2. Change the Local policy setting to *Do not allow enumeration of SAM accounts and shares*. Click OK.

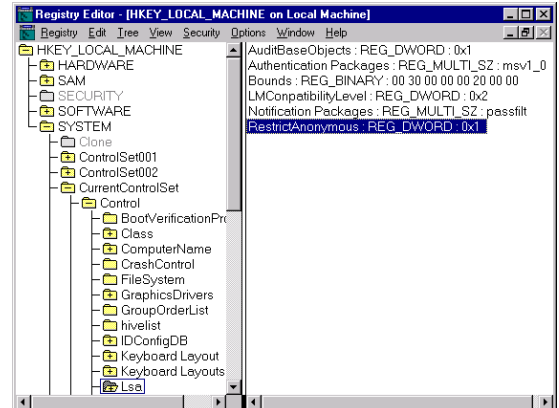


3. Close the Local Security Policy MMC by clicking the X in the upper right hand corner of the window. Closing this window evokes the change and is analogous to a system restart as normally required on NT 4.0 systems.
4. Reopen the Local Security Policy MMC and confirm that the effective policy setting is *Do not allow enumeration of SAM accounts and shares*.

Module 9 Lab Host System Hardening

B. If you are using an Windows NT 4.0 system, follow the below steps:

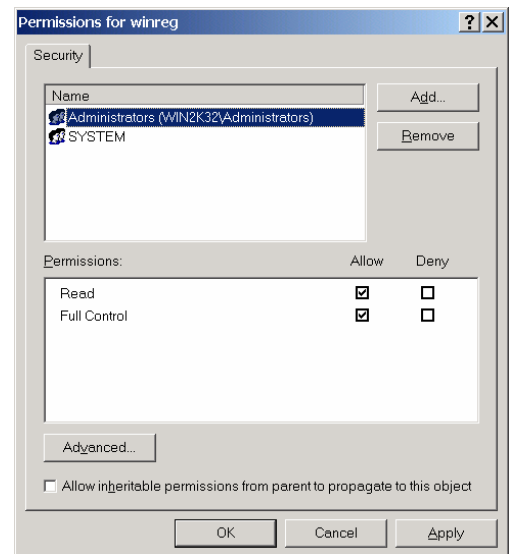
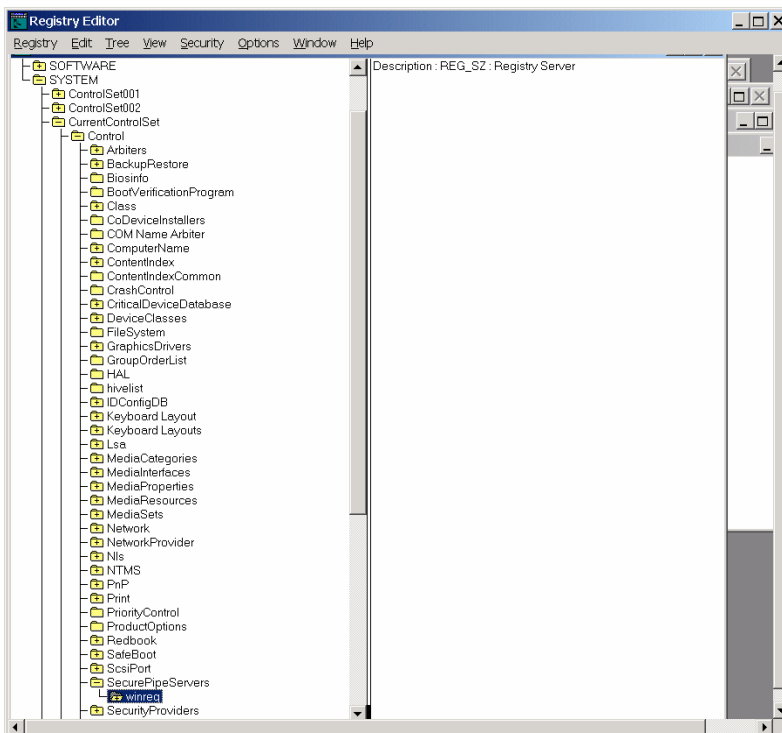
1. Click Start\Run and type *Regedt32*; this brings up the NT Registry Editor
2. Click on the HKEY_LOCAL_MACHINE (HKLM) window
3. Browse to the System\CurrentControlSet\Control\Lsa
4. Double Click on the *Restrict Anonymous* Registry Dword and change the Data value: to 1



Exercise 3 – Limit Remote Registry Access

To prevent unauthorized users from remotely editing the registry, take the following steps for either Windows NT/2000:

1. Click Start\Run and type *Regedt32*; this brings up the NT Registry Editor
2. Browse to HKLM\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg
3. Highlight the winreg key then click the Security Menu and select permissions
4. Set (ensure) this key so that only Administrators and System have remote access to the registry.
5. Depending on which Service Packs are loaded on the system, this may already be hardened.



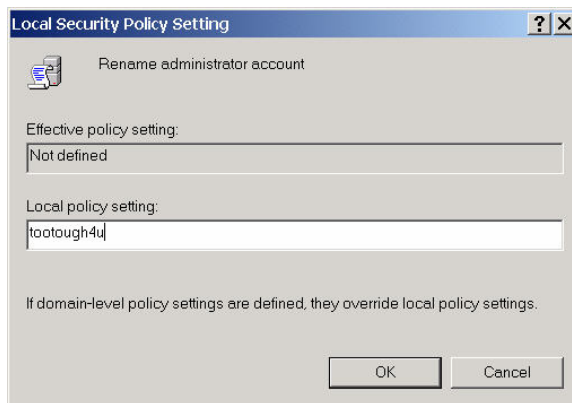
Exercise 4 – Harden Default Accounts

The Administrator account is built in (by default) on every copy of Windows NT/2000. This presents a well-known objective for attackers as they have half of the information needed for access—they only have to guess the correct password.

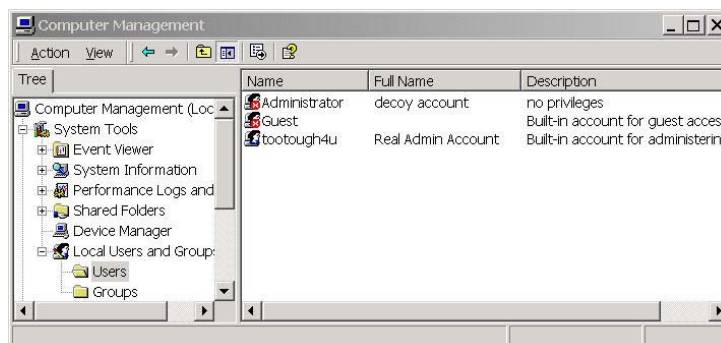
- To make it more difficult for potential intruders:
 - Rename the default Administrator account
 - Establish a decoy Administrator account with no privileges
 - Disable the decoy Administrator account

A. If you are using a Windows 2000 machine (NT 4.0 skip to B), follow the below steps:

1. Click Start/Settings/Control Panel/Administrative Tools/Local Security Policy. Under Local Policies, Security Options, double click *Rename administrator account*
2. Change the Local policy setting to a name that is obscure and not easily guessed—account names are not case sensitive!



3. From the desktop, Right click My Computer and select Manage
4. Under Local Users and Groups, right click on Users and select New User
5. Type *Administrator* as the User name, *decoy account* as the full name, and *no privileges* as the description and then click Create
6. Double click on the newly created account and click the Account is disabled check box
7. Click the Member Of tab, remove all groups in the dialogue box and then click OK



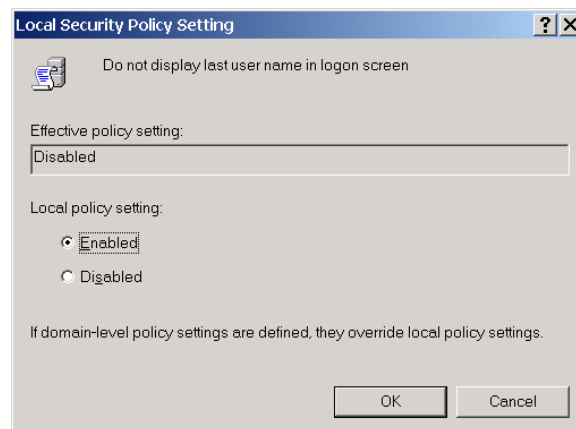
Module 9 Lab Host System Hardening

- B. If you are using Windows NT 4, follow the below steps:
1. Open User Manager (for Domains on NT Server) from the Start\Programs\Administrative Tools (Common) menu.
 2. Highlight the Administrator account and select File/Rename
 3. Use User Manager to add a new decoy Administrator account with no privileges, then disable this account (same process as for Windows 2000)

Exercise 5 – Hide Last Logged in User

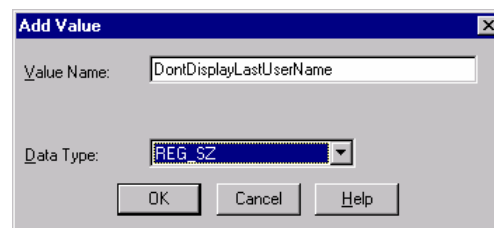
Showing a valid username in the User Login box gives away 50% of the required information to potential intruders.

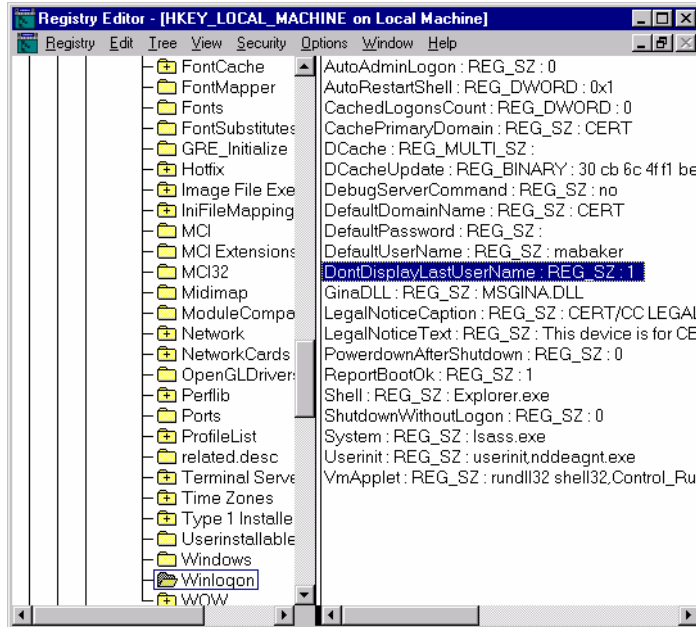
1. The last user logged in can be hidden using the MMC under Local Policies/Security Options, “Do not display last user name in logon screen”.



2. To hide the last logged in user in NT, make the following Registry change:
 - a. Start **Regedt32.exe** and locate the following registry key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
```
 - b. Add a REG_SZ value named *DontDisplayLastUserName* by clicking Edit/Add Value; then click OK. If a String dialogue box appears type *1*

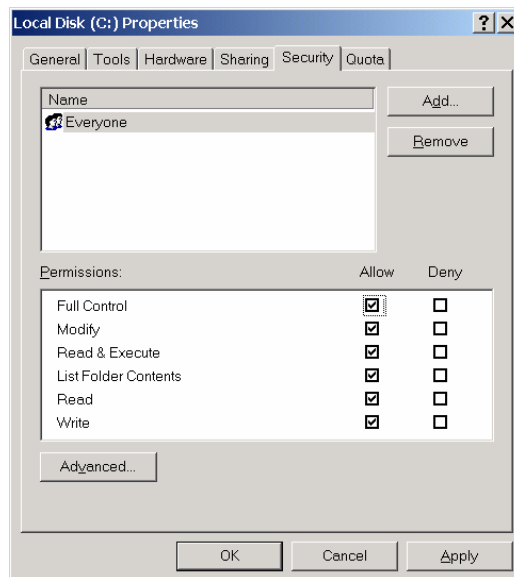




Exercise 6 – Changing Default Permissions

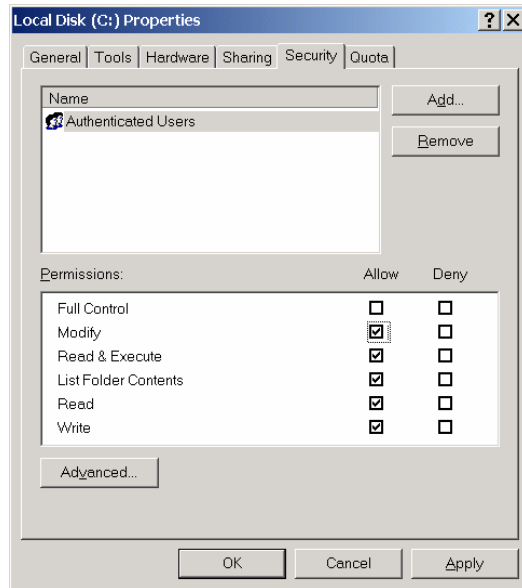
In Windows 2000 and NT, the C: drive's default permissions are Everyone/Full control. This should be changed to Authenticated Users only (or more restrictive).

1. To make this change, under My Computer right click on C: and go to the Security tab.



2. Remove the group Everyone and add the Authenticated Users group.

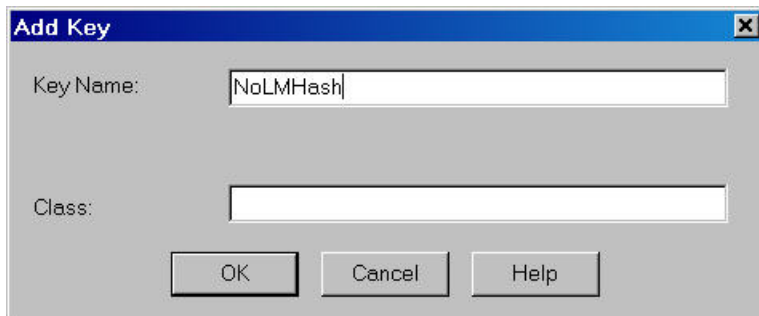
Module 9 Lab Host System Hardening



3. Authenticated Users will probably not need Full Control, but select other permissions as appropriate.


Exercise 7 – Eliminate storage of LanManager Hash (Windows 2000 SP2> only)

1. Click **Start|Run** and Type **Regedt32.exe** and hit enter
2. Browse to this key in the registry:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa
3. On the **Edit** Menu, click **Add Key**, type **NoLMHash**, and then click **OK**



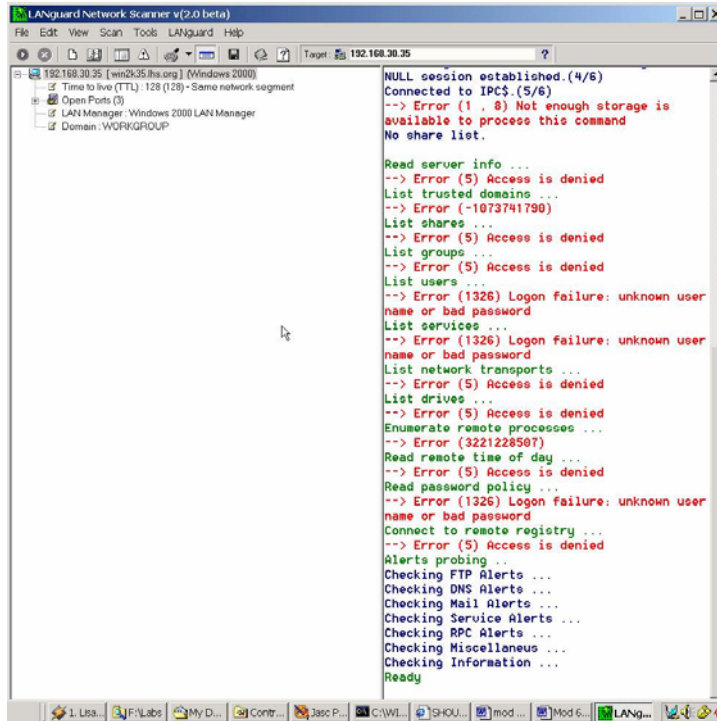
4. Exit Registry Editor
5. Restart Computer to make setting active
6. Change the Password of the Administrator account
7. Run LC3 against the administrator account and notice that the LM Hash field is blank

Exercise 8 – Test the new configurations

1. Open Languard Network Scanner again
2. Scan your partner's machine again (enter his/her IP address in the Target area and click the play button () to begin the scan

Module 9 Lab Host System Hardening

3. Notice the output now – and compare this to the output of the first scan. There are no shares shown, and much of the rest of the information has now not been enumerated.



```
LANguard Network Scanner v(2.0 beta)
File Edit View Scan Tools LANguard Help
Target: 192.168.30.35
192.168.30.35 [win2k35.lisa.org] (Windows 2000)
  Time to live (TTL): 128 (128) - Same network segment
  Open Ports (2)
  LAN Manager: Windows 2000 LAN Manager
  Domain: WORKGROUP
NULL session established.(4/6)
Connected to IPC$. (5/6)
--> Error (1, 8) Not enough storage is
available to process this command
No share list.

Read server info ...
--> Error (5) Access is denied
List trusted domains ...
--> Error (-1073741790)
List shares ...
--> Error (5) Access is denied
List groups ...
--> Error (5) Access is denied
List users ...
--> Error (1326) Logon failure: unknown user
name or bad password
List services ...
--> Error (1326) Logon failure: unknown user
name or bad password
List network transports ...
--> Error (5) Access is denied
List drives ...
--> Error (5) Access is denied
Enumerate remote processes ...
--> Error (3221228507)
Read remote time of day ...
--> Error (5) Access is denied
Read password policy ...
--> Error (1326) Logon failure: unknown user
name or bad password
Connect to remote registry ...
--> Error (5) Access is denied
Alerts probing ..
Checking FTP Alerts ...
Checking DNS Alerts ...
Checking Mail Alerts ...
Checking Service Alerts ...
Checking RPC Alerts ...
Checking Miscellaneous ...
Checking Information ...
Ready
```